Dynamix UM-SB Series

G.SHDSL .bis Router

User Manual

Version 0.06

Table of Contents

1 Descriptions

The Dynamix UM-SB (Symmetric High Speed Digital Subscriber Loop) router (with ATM/EFM layer) comply with G.991.2(2004) standard optimized for small to medium size business environment. It provides business-class, multi-range from 192Kbps to 5.696Mbps (for 2-wire model) and 384Kbps to 11.392Mbps (for 4-wire model) symmetric payload rates over exiting copper wire. The various pair bonding techniques make it suitable for any types of DSL infrastructure.

The SHDSL.bis routers are integrated high-end Bridging/Routing capabilities with advanced functions of Multi-DMZ, virtual server mapping, VPN pass-through and QoS.

Because of rapid growth of network, virtual LAN has become one of the major new areas in internetworking industry. The SHDSL.bis routers supports the port-based and IEEE 802.1q VLAN over ATM network or EFM network.

The SHDSL.bis routers support 10Base-T /100Base-T auto-negotiation and auto-MDI/MDIX switching port to meet the enterprise need.

The firewall routers models provides advanced firewall with DoS protection, serving as a powerful firewall to protect from outside intruders of secure connection. The firewall routers also support IP precedence to classify and prioritize types of IP traffic.

The 4-port routers models support four ports 10Base-T /100Base-T auto-negotiation and auto-MDI/MDIX switching ports to meet the enterprise need.

The SHDSL.bis routers allow customers to leverage the latest in broadband technologies to meet their growing data communication needs. User can gradually migrate from ATM based access networks to Ethernet based access networks. This means that this device can be installed in an existing ATM network. When the network migrates to Ethernet, the same this device can re-used in the Ethernet network without on-site intervention. The unique feature of combining ATM and EFM access in the same device leverages a smooth migration of the access network.

1.1 Features

- ✓ Easy configuration and management with password control for various application environments
- ✓ Efficient IP routing and transparent learning bridge to support broadband Internet services
- ✓ VPN pass-through for safeguarded connections
- ✓ Virtual LANs (VLANs) offer significant benefit in terms of efficient use of bandwidth, flexibility, performance and security
- ✓ Build-in advanced SPI firewall (Firewall router)
- ✓ Four 10/100Mbps Auto-negotiation and Auto-MDI/MDIX switching port for flexible local area

network connectivity (4-port router)

- ✓ DMZ host/Multi-DMZ/Multi-NAT enables multiple workstations on the LAN to access the Internet for the cost of IP address
- ✓ Fully ATM protocol stack implementation over SHDSL.bis
- ✓ IEEE 802.3 2BASE-TL for EFM operation
- ✓ PPPoA and PPPoE support user authentication with PAP/CHAP/MS-CHAP
- ✓ SNMP management with SNMPv1/SNMPv2 agent and MIB II
- ✓ Getting enhancements and new features via Internet software upgrade

1.2 Specification

Routing

- Support IP/TCP/UDP/ARP/ICMP/IGMP protocols
- IP routing with static routing and RIPv1/RIPv2 (RFC1058/2453)
- IP multicast and IGMP proxy (RFC1112/2236)
- Network address translation (NAT/PAT) (RFC1631)
- NAT ALGs for ICQ/NetMeeting/MSN/Yahoo Messenger
- DNS relay and caching (RFC1034/1035)
- DHCP server, client and relay (RFC2131/2132)
- IP precedence (RFC 791) (Firewall model)

Bridging

- Up to 1024 MAC address learning bridge
- IEEE 802.1q VLAN, IEEE 802.1D STP
- Port-based VLAN (4-port model)
- Spanning tree protocol

Security

- DMZ host/Multi-DMZ/Multi-NAT function
- Virtual server mapping (RFC1631)
- VPN pass-through for PPTP/L2TP/IPSec tunneling
- Natural NAT firewall
- Application level gateway for URL and keyword blocking (Firewall model)
- User access control: deny certain access of PCs to Internet service (Firewall model)

Management

- Easy-to-use web-based GUI for quick setup, configuration and management
- Menu-driven interface/Command-line interface (CLI) for local console and Telnet access
- Password protected management and access control list for administration

- SNMP management with SNMPv1/SNMPv2 (RFC1157/1901/1905) agent and MIB II (RFC1213/1493)
- Software upgrade via web-browser/TFTP server
- Support detailed logging via Syslog.
-

ATM

- Up to 8 PVCs
- OAM F5 AIS/RDI and loopback
- AAL5

ATM QoS

- UBR (Unspecified bit rate)
- CBR (Constant bit rate)
- VBR-rt (Variable bit rate real-time)
- VBR-nrt (Variable bit rate non-real-time)

AAL5 Encapsulation

- VC multiplexing and SNAP/LLC
- Ethernet over ATM (RFC 2684/1483)
- PPP over ATM (RFC 2364)
- Classical IP over ATM (RFC 1577)

PPP

- PPP over Ethernet for fixed and dynamic IP (RFC 2516)
- PPP over ATM for fixed and dynamic IP (RFC 2364)
- User authentication with PAP/CHAP/MS-CHAP

WAN Interface

- SHDSL.bis: ITU-T G.991.2 (2004)
- Annex A, B, AF, and BG supported
- SHDSL.bis encoding scheme: 16-TCPAM and 32-TCPAM
- EFM 2BASE-TL 64/65-octet encoding
- EFM bonding: IEEE 802.3ah PAF
- Data Rate: N x 64Kbps ,N=3~89 (for 2-wire model)
- Data Rate: N x 128kbps, N= 3~89 (for 4-wire model)
- Impedance: 135 ohms

Virtual LAN

- 802.1Q Tag-Based VLAN
- Port Based VLAN

LAN Interface

- 4-ports switching hub (4-port model)
- 10/100 Base-T auto-sensing and auto-negotiation
- Auto-MDI/MDIX

Hardware Interface

- WAN: RJ-45
- LAN: RJ-45 x 4 (4-port model) or RJ-45 x 1 (1-port model)
- Console: RS232 female
- Reset Button: Reset button for factory default

Indicators

- General: PWR
- WAN: LNK, ACT
- LAN: 10M/ACT, 100M/ACT (for1-port model)
- LAN: 1, 2, 3, 4 (for 4-port model)
- SHDSL.bis: ALM

Physical/Electrical

- Dimensions: 18.7 x 3.3 x 14.5cm (WxHxD)
- Power: 100~240VAC (via power adapter)
- Power consumption: 9 watts maximum.
- Temperature: 0~45°C
- Humidity: 0%~95%RH (non-condensing)

Memory

- 2MB Flash Memory, 8MB SDRAM

Products' Information

✧ UM-SB 2-wire router/bridge with 1-port LAN

✧ UM-SFB 2-wire router/bridge with 1-port LAN, VLAN and business class firewall

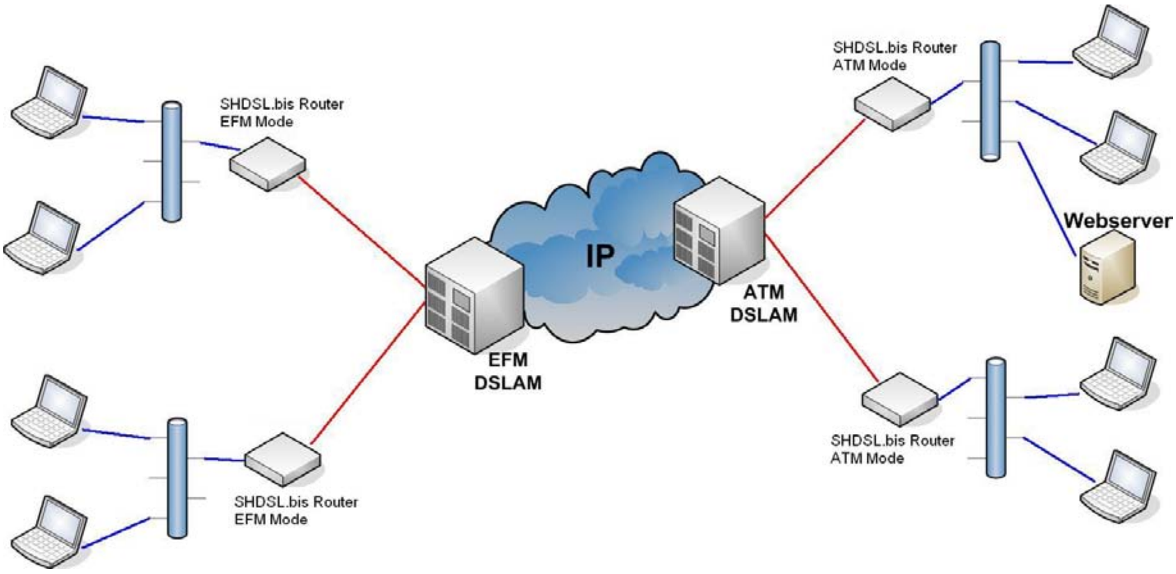
✧ UM-S4B 2-wire router/bridge with 4-ports switching hub LAN, VLAN

✧ UM-S4FB 2-wire router/bridge with 4-ports switching hub LAN, VLAN and business class firewall

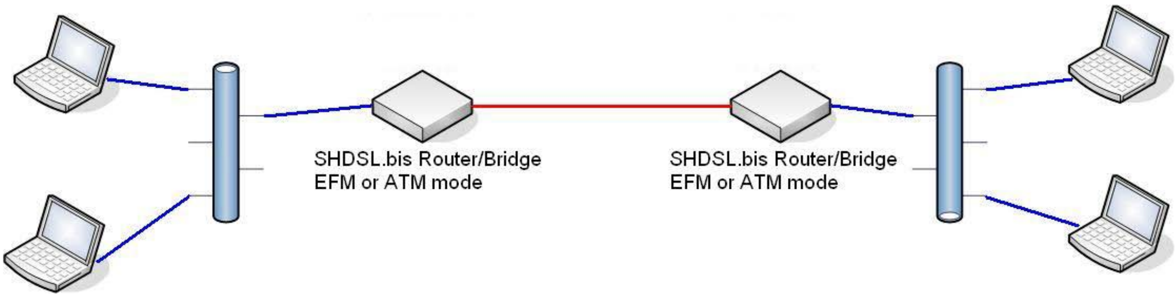
✧ UM-S4B/4W 4-wire router/bridge with 4-ports switching hub LAN, VLAN

✧ UM-S4FB/4W 4-wire router/bridge with 4-ports switching hub LAN, VLAN and business class firewall

1.3 Applications



Combination with EFM or ATM DSLAM



Point-to-point connection

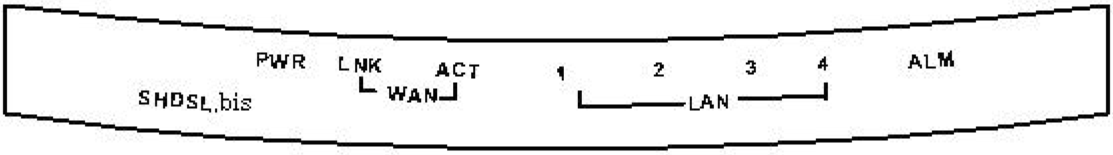
.

2 Getting to know about the router

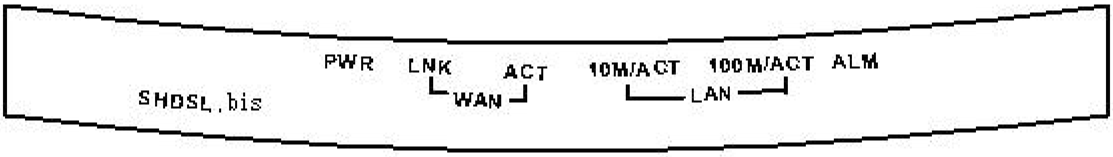
This section will introduce hardware of the router.

2.1 Front Panel

The front panel contains LEDs which show status of the router.



Front Panel of SHDSL .bis 4-port router/bridge



Front Panel of SHDSL.bis 1-port router/bridge

LED status of SHDSL.bis 4-ports router

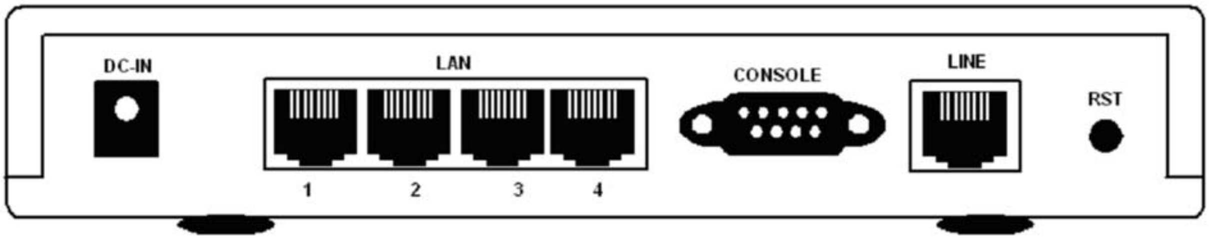
LEDs		Active	Description
PWR		On	Power on
WAN	LNK	On	SHDSL.bis line connection is established
		Blink	SHDSL.bis handshake
	ACT	On	Transmit or received data over SHDSL.bis link
LAN	1	On	Ethernet cable is connected to LAN 1
		Blink	Transmit or received data over LAN 1
	2	On	Ethernet cable is connected to LAN 2
		Blink	Transmit or received data over LAN 2
	3	On	Ethernet cable is connected to LAN 3
		Blink	Transmit or received data over LAN 3
	4	On	Ethernet cable is connected to LAN 4
		Blink	Transmit or received data over LAN 4
ALM		On	SHDSL.bis line connection is dropped
		Blink	SHDSL.bis self test

LED status of SHDSL.bis 1-port router

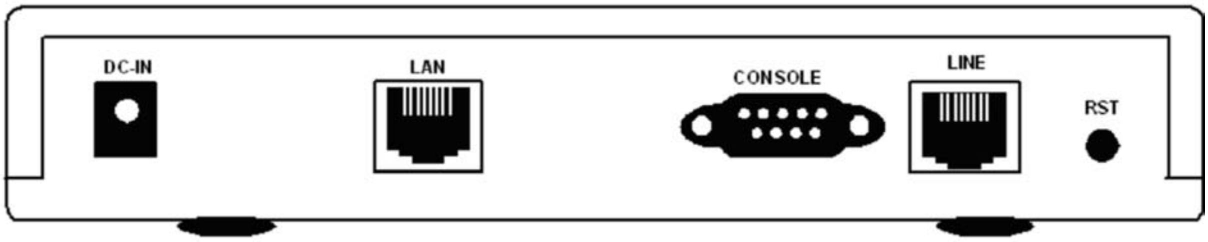
LEDs		Active	Description
PWR		On	Power adaptor is connected to the router
WAN	LNK	On	SHDSL.bis line connection is established
		Blink	SHDSL.bis handshake
	ACT	Blink	Transmit or received data over SHDSL.bis link
LAN	10M/ACT	On	LAN port connect with 10M NIC
		Blink	LAN port acts in 10M
	100M/ACT	On	LAN port connect with 100M NIC
		Blink	LAN port acts in 100M
ALM		On	SHDSL.bis line connection is dropped
		Blink	SHDSL.bis self test

2.2 Rear Panel

The rear panel of SHDSL.bis router is where all of the connections are made.



Rear Panel of SHDSL.bis 4-wire/2-wire,4-port router/bridge



Rear Panel of SHDSL.bis 2-wire/1-port router/bridge

Connectors Description of SHDSL.bis 4-ports router

DC-IN	Power adaptor inlet: Input voltage 9VDC
LAN (1,2,3,4)	Four Ethernet10/100BaseT auto-sensing and auto-MDI/MDIX for LAN ports(RJ-45)
CONSOLE	RS- 232C (DB9) for system configuration and maintenance
LINE	SHDSL.bis interface for WAN port (RJ-45)
RST	Reset button for reboot or load factory default

Connectors Description of SHDSL.bis 1-port router

DC-IN	Power adaptor inlet: Input voltage 9VDC
LAN	Ethernet 10/100BaseT auto-sensing and auto-MDI/MDIX for LAN port (RJ-45)
CONSOLE	RS- 232C (DB9) for system configuration and maintenance
LINE	SHDSL.bis interface for WAN port (RJ-45)
RST	Reset button for reboot or load factory default

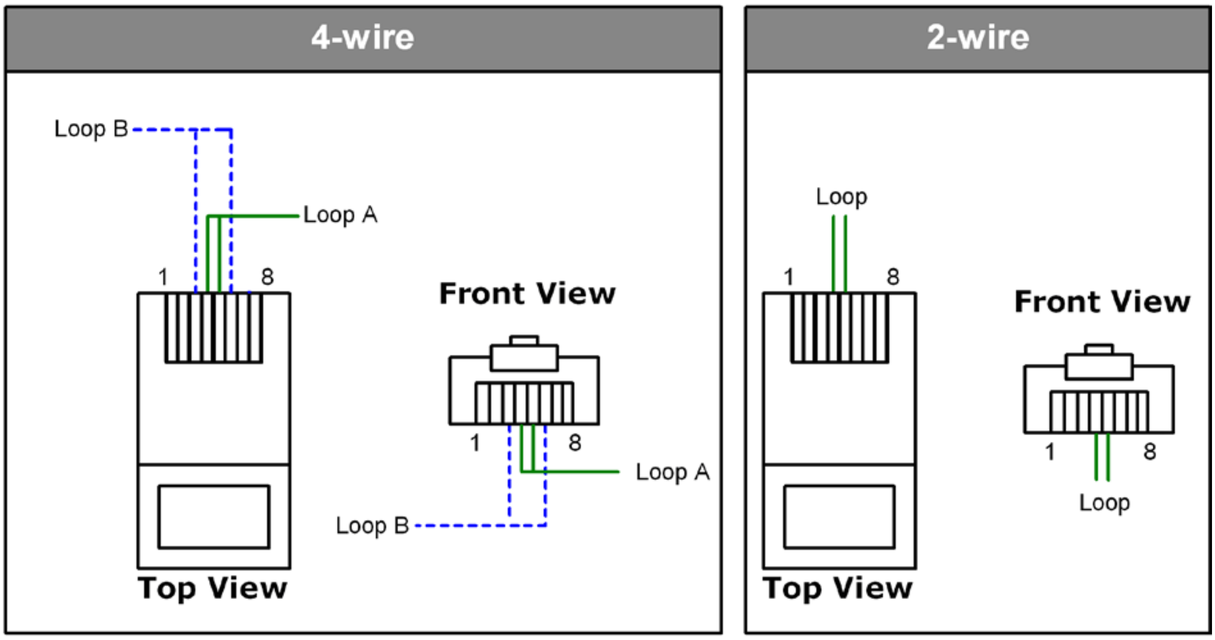
The reset button can be used only in one of two ways.

(1) Press the Reset Button for one second will cause system reboot.

(2) Pressing the Reset Button for four seconds will cause the product loading the factory default setting and losing all of yours configuration. When you want to change its configuration but forget the user name or password, or if the product is having problems connecting to the Internet and you want to configure it again clearing all configurations, press the Reset Button for four seconds with a paper clip or sharp pencil.

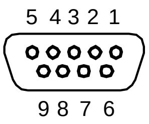
2.3 SHDSL.bis Line Connector

Below figure show the SHDSL.bis line cord plugs pin assignment:



2.4 Console Cable

Below figure show the cosole cable pins asignment:

Pin Number	Description	Figure
1	No connection	
2	RxD (O)	
3	TxD (I)	
4	No connection	
5	GND	
6	No connection	
7	CTS (O)	
8	RTS (I)	
9	No connection	

3 Install to the Router

This guide is designed to let users through Web Configuration or serial console with G.shdsl.bis Router in the easiest and quickest way possible. Please follow the instructions carefully.

Note: There are three methods to configure the router: serial console, Telnet and Web Browser. Only one configuration application is used to setup the Router at any given time. Users have to choose one method to configure it.
For Web configuration, you can skip item 3.
For Serial Console Configuration, you can skip item 1 and 2.

3.1 Check List

(1) Check the Ethernet Adapter in PC or NB

Make sure that Ethernet Adapter had been installed in PC or NB used for configuration of the router. TCP/IP protocol is necessary for web configuration, so please check the TCP/IP protocol whether it has been installed.

(2) Check the Web Browser in PC or NB

According to the Web Configuration, the PC or NB need to install Web Browser, IE or Netscape.
Note: Suggest to use IE5.0, Netscape 6.0 or above and 800x600 resolutions or above.

(3) Check the Terminal Access Program

For Serial Console and Telnet Configuration, users need to setup the terminal access program with VT100 terminal emulation.

(4) Determine Connection Setting

Users need to know the Internet Protocol supplied by your Service Provider and determine the mode of setting.

Protocol Selection

RFC1483	Ethernet over ATM
RFC1577	Classical Internet Protocol over ATM
RFC2364	Point-to-Point Protocol over ATM
RFC2516	Point-to-Point Protocol over Ethernet

The difference Protocols need to setup difference WAN parameters. After knowing the Protocol provided by ISP, you have to ask the necessary WAN parameters to setup it.

Bridge EoA

VPI:_
VCI:__
Encapsulation:
Gateway:
Host Name:(if applicable)

Route EoA

VPI:_
VCI:__
Encapsulation:
IP Address:
Subnet Mask:_
Gateway:
DNS Server:_

IPoA

VPI:_
VCI:__
Encapsulation:
IP Address:
Subnet Mask:_
Gateway:
DNS Server:_

PPPoA

VPI:_
VCI:__
Encapsulation:
User Name:
Password:
DNS Server:_
Host Name: (if applicable)

PPPoE

VPI:_
VCI:__
Encapsulation:
User Name:
Password:
DNS Server:_
Host Name:(if applicable)

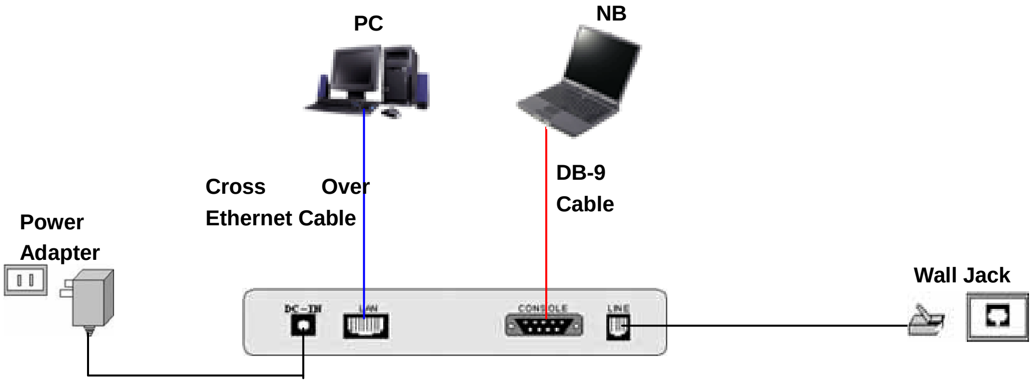
3.2 Install the SHDSL.bis Router

⚠

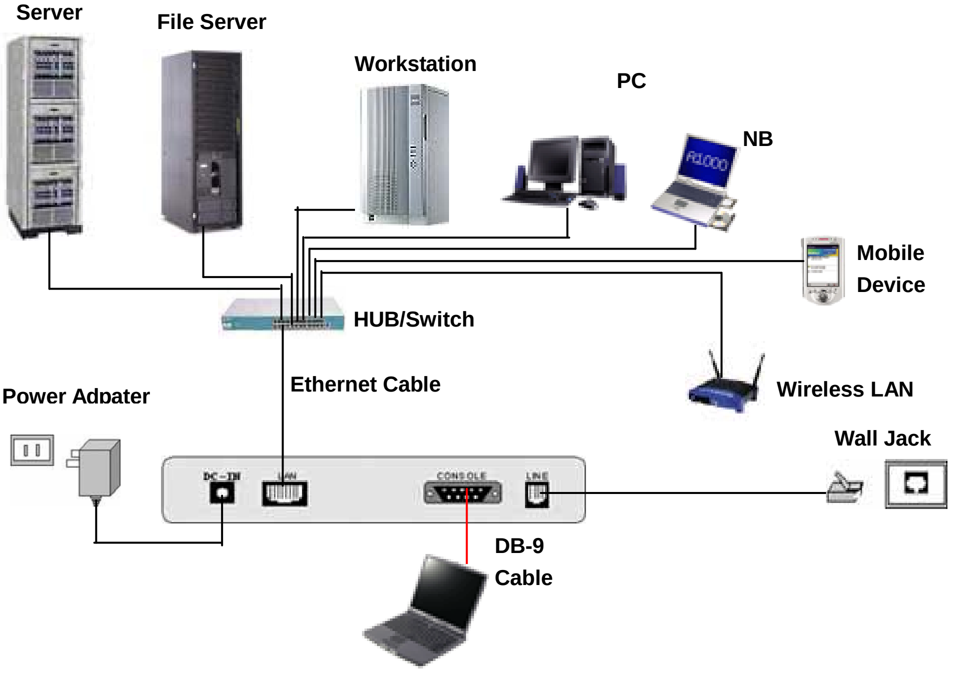
To avoid possible damage to this Router, do not turn on the router before Hardware Installation.

- Connect the power adapter to the port labeled DC-IN on the rear panel of the product.
- Connect the Ethernet cable.

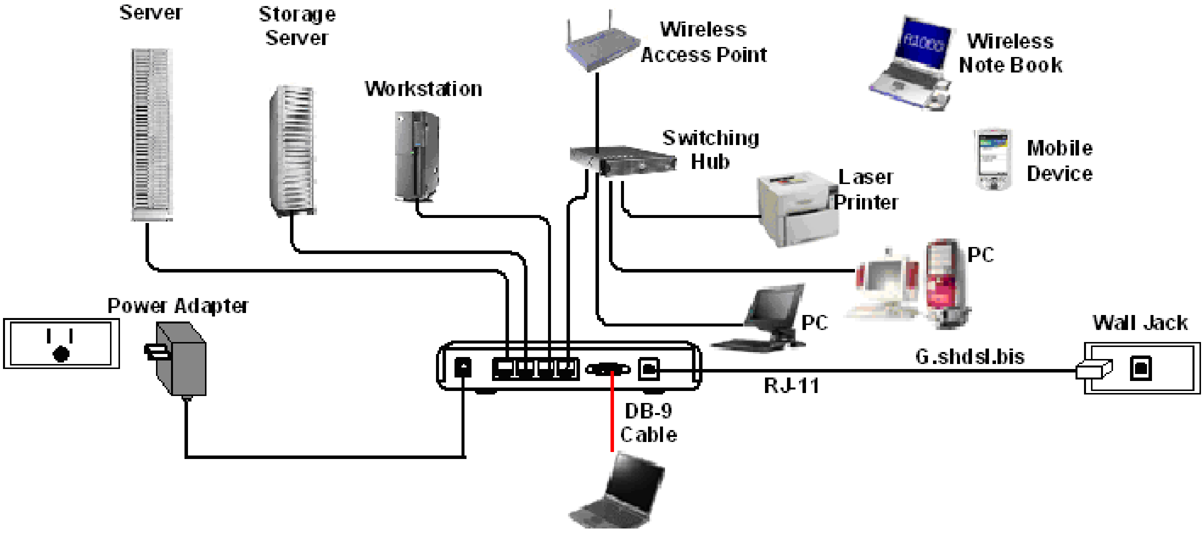
  Note: Both the 1-port router and 4-ports router supports auto-MDI/MDIX switching so both straight through and cross-over Ethernet cable can be used.
- Connect the phone cable to the router and the other side of phone cable to wall jack.
- Connect the power adapter to power source inlet.
- Turn on the PC or NB, which is used for configuration the Router.



Direct Connection with PC or NB for SHDSL.bis 1-port router



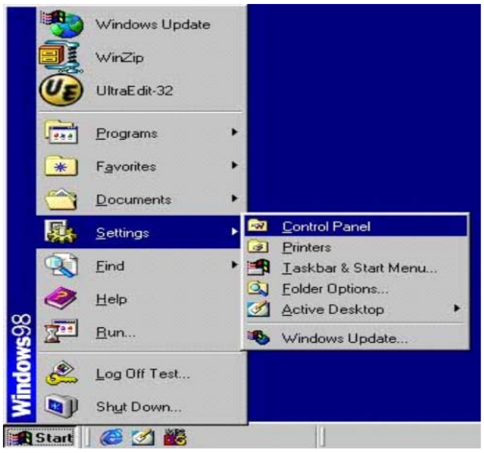
Connection with Hub/Switch for SHDSL.bis 1-port router



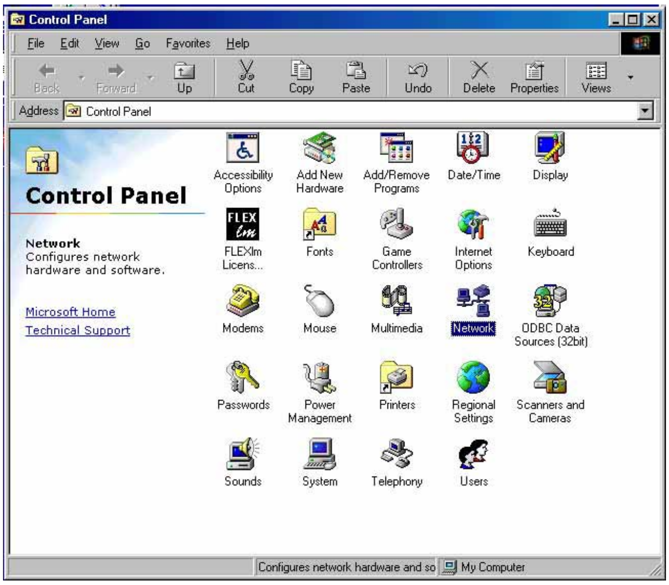
SHDSL.bis 4-ports router with complex network topology

4 Configuration via Web Browser

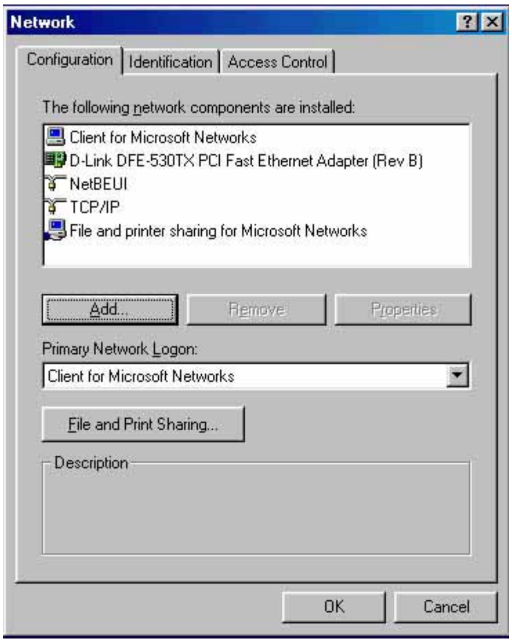
Step. 1 Click the **start** button. Select **setting** and **control panel**.



Step. 2 Double click the **network** icon.



In the Configuration window, select the **TCP/IP** protocol line that has been associated with your network card and then click **property** icon.

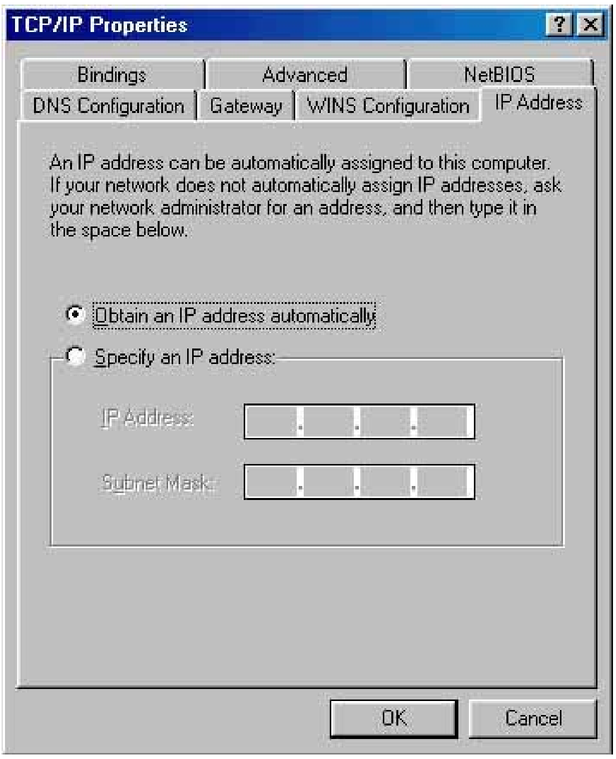


The following network components are installed:

- Client for Microsoft Networks
- D-Link DFE-530TX PCI Fast Ethernet Adapter (Rev B)
- NetBEUI
- TCP/IP
- File and printer sharing for Microsoft Networks

Primary Network Logon: Client for Microsoft Networks

Choose IP address tab.
Select **Obtain IP address automatically**.
Click **OK** button.

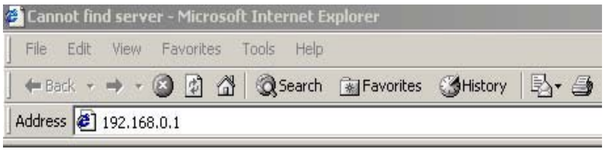


An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

○ Specify an IP address:

The window will ask you to restart the PC. Click **Yes** button.

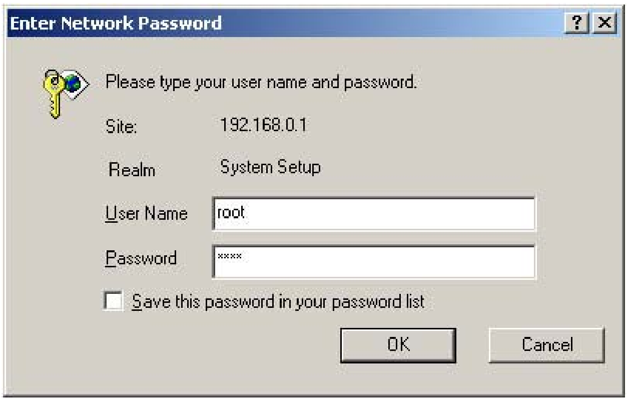

Cannot find server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address

192.168.0.1

After rebooting your PC, open IE or Netscape Browser to connect the Router. Type

http://192.168.0.1

The default IP address and sub net-mask of the Router is 192.168.0.1 and 255.255.255.0. Because the router acts as DHCP server in your network, the router will automatically assign IP address for PC or NB in the network.



Site: 192.168.0.1

Realm System Setup

User Name root

Password ****

□ Save this password in your password list

Type User Name root and Password root and then click OK.
The default user name and password both is *root*. For the system security, suggest changing them after configuration.

Note: After changing the User Name and Password, strongly recommend you to save them because another time when you login, the User Name and Password have to be used the new one you changed.

Function Listing

Following is the G.SHDSL.bis router full function listing.

- **BASIC (Quick Setup)**
- **ADVANCED**
  - SHDSL.bis
  - WAN
  - BRIDGE
  - VLAN
  - STP
  - ROUTE
  - NAT/DMZ
  - VIRTUAL SERVER
  - FIREWALL
  - IP QoS
- **STATUS**
  - SHDSL.bis
  - LAN
  - WAN
  - ROUTE
  - INTERFACE
  - FIREWALL
  - IP QoS
  - STP
- **ADMIN**
  - SECURITY
  - SNMP
  - SYSLOG
  - TIME SYNC
- **UTILITY**
  - SYSTEM INFO
  - SYSLOG
  - CONFIG TOOL
  - UPGRADE
  - LOGOUT
  - RESTART

Note:

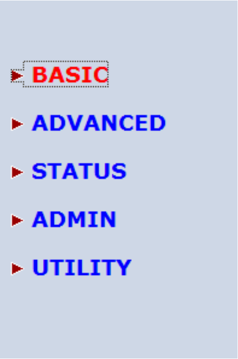
If the router is not the Firewall model, the menu will not display FIREWALL items.

If the router is not the 4-wires model, the menu will not display the status of SHDSL.bis channel B.

4.1 Basic Setup

The Basic Setup contains Bridge or Route operation mode. User can use it to completely setup the router. After successfully completing it, you can access Internet or as LAN extension. This is the easiest and possible way to setup the router.

Note: The advanced functions are only for advanced users to setup advanced functions. The incorrect setting of advanced function will affect the performance or system error, even disconnection.



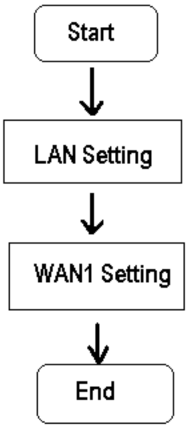
Click Basic for basic installation.

4.1.1 Bridge Mode

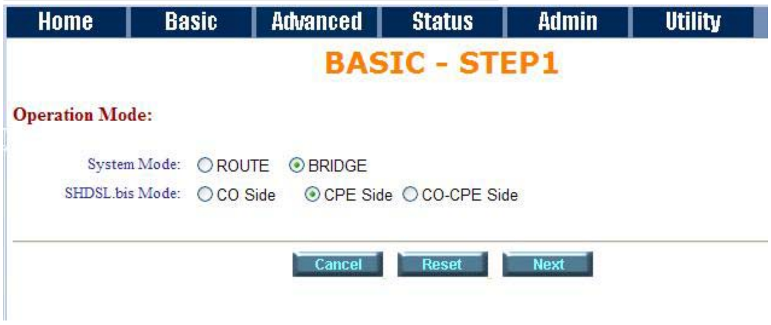
Parameter Table:

System mode	□Route ☒Bridge	
SHDSL	□CO side □CPE side □CO-CPE side	
LAN	IP address	
	Subnet Mast	
	Gateway	
	Host Name	
WAN1	VPI	
	VCI	
	Encapsulation	□VC-mux □LLC

The flow chart of bridge mode setup:



Setup up system mode and SHDSL mode



BASIC - STEP1

Operation Mode:

System Mode: ○ ROUTE ● BRIDGE

SHDSL.bis Mode: ○ CO Side ● CPE Side ○ CO-CPE Side

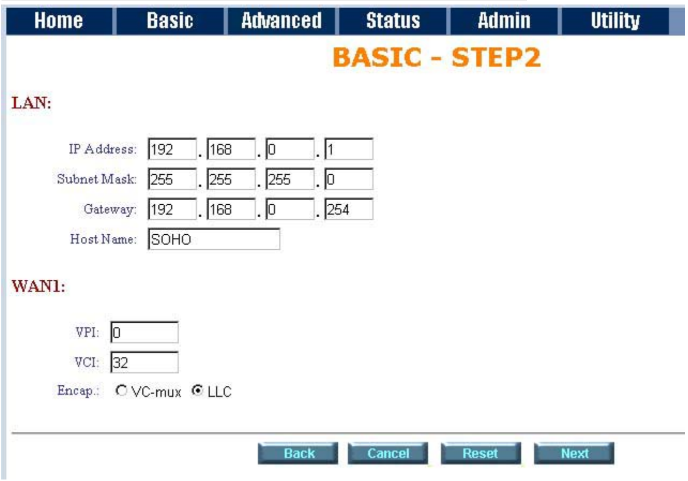
Click Bridge and CPE Side to setup Bridging mode and then click Next for the next setting.

This router can be setup as one of two SHDSL.bis working mode: CO (Central Office) and CPE (Customer Premises Equipment).

The CO-CPE Side only for Multi-link mode of 4-wires model. Channel A is used as CO side and channel B is used as CPE side.

For connection with DSLAM, the SHDSL.bis router's working mode is CPE. For "LAN to LAN" connection, one side must be CO and the other side must be CPE.

Set up (a) LAN IP address , Subnet Mask, Gateway and Host Name
(b) WAN1 VPI,VCI and Encapsulation



BASIC - STEP2

LAN:

IP Address: 192 . 168 . 0 . 1

Subnet Mask: 255 . 255 . 255 . 0

Gateway: 192 . 168 . 0 . 254

Host Name: SOHO

WAN1:

VPI: 0

VCI: 32

Encap.: ○ VC-mux ● LLC

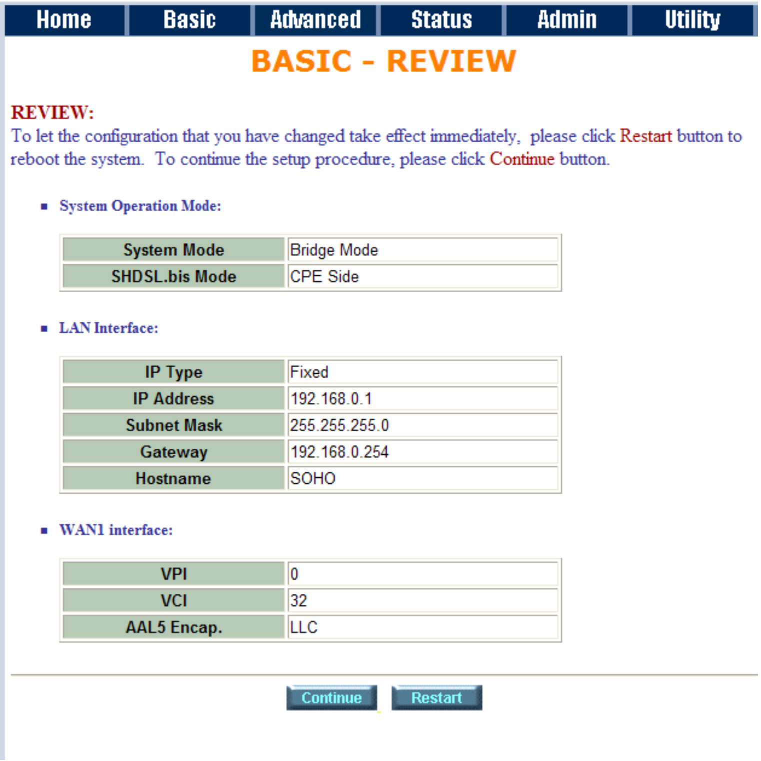
LAN:

IP: 192.168.0.1
Subnet Mask: 255.255.255.0
Gateway: 192.168.0.254 (The Gateway IP is provided by ISP.)
Host Name: SOHO

Some of the ISP requires the Host Name as identification. You may check with ISP to see if your Internet service has been configured with a host name. In most cases, this field can be ignored.

WAN1:
VPI: 0
VCI: 32
Encap: Click LLC and than Click Next to review

Review



BASIC - REVIEW

REVIEW:
To let the configuration that you have changed take effect immediately, please click Restart button to reboot the system. To continue the setup procedure, please click Continue button.

- System Operation Mode:

System Mode	Bridge Mode
SHDSL.bis Mode	CPE Side

- LAN Interface:

IP Type	Fixed
IP Address	192.168.0.1
Subnet Mask	255.255.255.0
Gateway	192.168.0.254
Hostname	SOHO

- WAN1 interface:

VPI	0
VCI	32
AAL5 Encap.	LLC

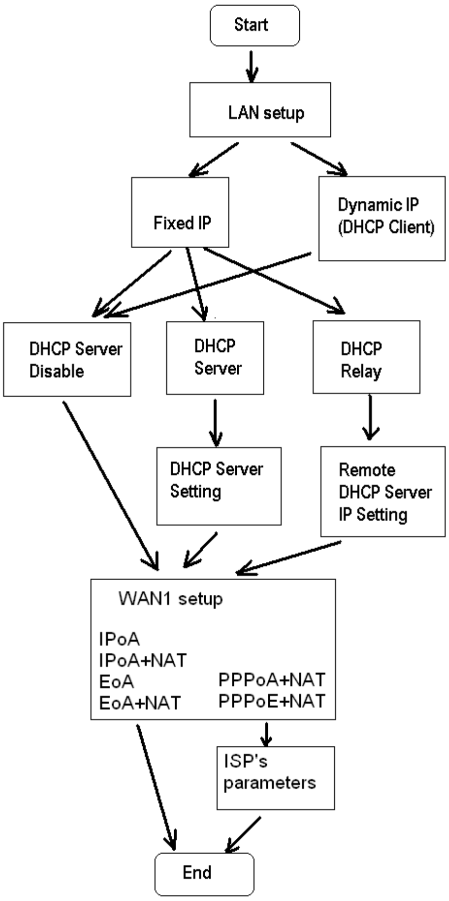
The screen will prompt the new configured parameters. When using on bridge mode, the protocol mode must be automatic set to Ethernet over ATM (EoA).Checking the parameters and Click Restart .The router will reboot with the new setting or Continue to configure another parameters.

4.1.2 Routing Mode

Parameter Table:

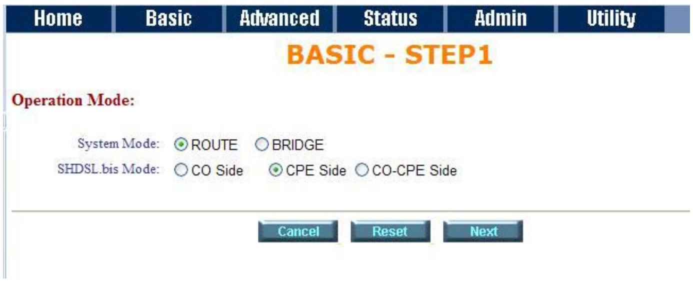
System mode	☒Route ☐Bridge			
SHDSL	☐CO side ☐CPE side ☐CO-CPE side			
LAN	IP type		☐Fixed ☐Dynamic(DHCP Client)	
	IP address			
	Subnet Mast			
	Host Name			
	Trigger DHCP service		☐Disable ☐Server ☐Relay	
WAN1	VPI			
	VCI			
	Encapsulation		☐VC-mux ☐LLC	
	Protocol		☐IPoA ☐IPoA + NAT ☐EoA ☐EoA + NAT ☐PPPoA + NAT ☐PPPoE + NAT	
DHCP Server	Default gateway			
	Subnet Mast			
	Start IP address			
	End IP address			
	DNS Server 1			
	DNS Server 2			
	DNS Server 3			
	Lease time			
	Host Entries	1	MAC :	IP:
		2	MAC :	IP:
		3	MAC :	IP:
		4	MAC :	IP:
		5	MAC :	IP:
		6	MAC :	IP:
		7	MAC :	IP:
		8	MAC :	IP:
		9	MAC :	IP:
		10	MAC :	IP:
DHCP Relay	IP address			

The flow chart of route mode setup:



Routing mode contains DHCP server, DHCP client, DHCP relay, Point-to-Point Protocol over ATM and Ethernet and IP over ATM and Ethernet over ATM. You have to clarify which Internet protocol is provided by ISP.

Setup up system mode and SHDSL mode



BASIC - STEP1

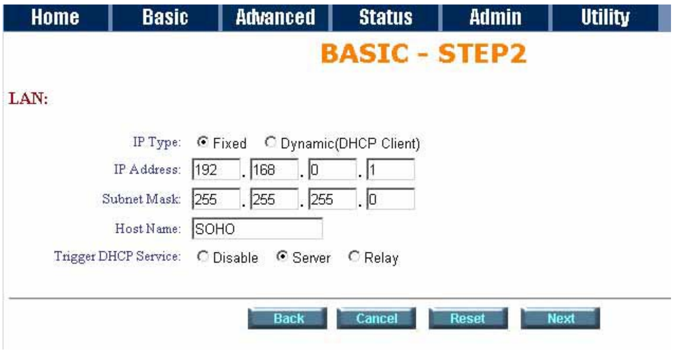
Operation Mode:

System Mode: ● ROUTE ○ BRIDGE

SHDSL.bis Mode: ○ CO Side ● CPE Side ○ CO-CPE Side

click ROUTE and CPE Side then press Next.

Set up the LAN IP address , Subnet Mask, Gateway, Host Name and Trigger DHCP Service with fixed IP type.



BASIC - STEP2

LAN:

IP Type: ● Fixed ○ Dynamic(DHCP Client)

IP Address: 192 . 168 . 0 . 1

Subnet Mask: 255 . 255 . 255 . 0

Host Name: SOHO

Trigger DHCP Service: ○ Disable ● Server ○ Relay

IP type: Fixed
IP Address: 192.168.0.1
Subnet Mask: 255.255.255.0
Host Name: SOHO
Some of the ISP requires the host name as identification. You may check with ISP to see if your Internet service has been configured with a host name. In most cases, this field can be ignored.

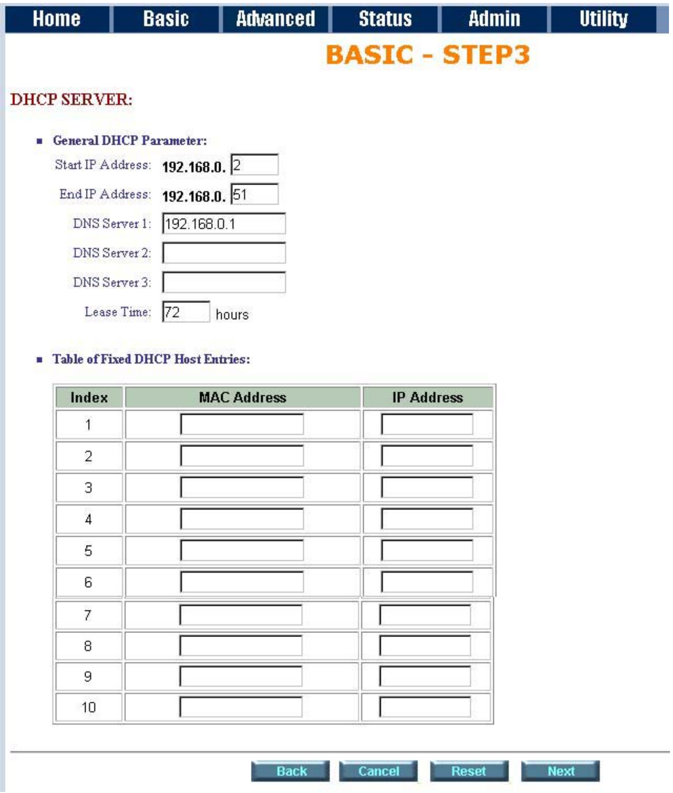
Trigger DHCP Service: Server
The default setup is Enable DHCP server. If you want to turn off the DHCP service, choose Disable.

If set DHCP server to Relay, the router acts as a surrogate DHCP server and relays requests and responses between the remote server and the clients.

DHCP Server
Dynamic Host Configuration Protocol (DHCP) is a communication protocol that lets network administrators to manage centrally and automate the assignment of Internet Protocol (IP) addresses in an organization's network. Using the Internet Protocol, each machine that can connect to the Internet needs a unique IP address. When an organization sets up its computer users with a connection to the Internet, an IP address must be assigned to each machine.
Without DHCP, the IP address must be entered manually at each computer. If computers move to another location in another part of the network, a new IP address must be entered. DHCP lets a network administrator to supervise and distribute IP addresses from a central point and automatically sends a new IP address when a computer is plugged into a different place in the network.

If the DHCP server is “Enable,” you have to setup the following parameters for processing it as DHCP server.
The embedded DHCP server assigns network configuration information at most 253 users accessing the Internet in the same time.

Set up the DHCP Server parameters and fixed DHCP host table



BASIC - STEP3

DHCP SERVER:

- General DHCP Parameter:

Start IP Address: 192.168.0. 2

End IP Address: 192.168.0. 51

DNS Server 1: 192.168.0.1

DNS Server 2:

DNS Server 3:

Lease Time: 72 hours

- Table of Fixed DHCP Host Entries:

Index	MAC Address	IP Address
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Start IP Address: This field specifies the first of the contiguous addresses in the IP address pool.
End IP Address: The field specifies the last of the contiguous addresses in the IP address pool.

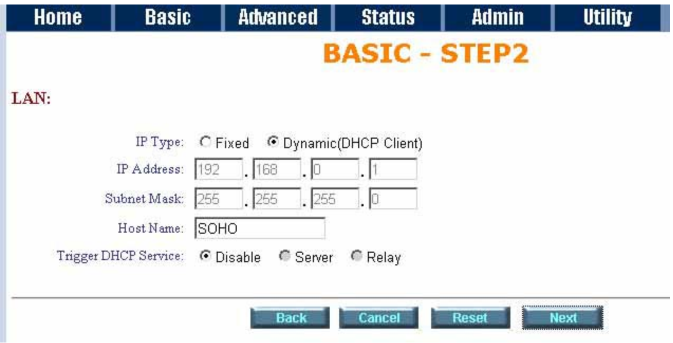
For example: If the LAN IP address is 192.168.0.1, the IP range of LAN is 192.168.0.2 to 192.168.0.51. The DHCP server assigns the IP form Start IP Address to End IP Address. The legal IP address range is form 0 to 255, but 0 are reserved as network name and 255 are reserved for broadcast. It implies the legal IP address range is from 1 to 254. That means you cannot assign an IP greater than 254 or less then 1. **Lease time** 72 hours indicates that the DHCP server will reassign IP information in every 72 hours.

DNS Server1, **DNS Server2** and **DNS Server3**: Your ISP will provide at least one Domain Name Service Server IP. You can type the router IP in this field. The router will act as DNS server relay function. There have three DNS server can use.
You may assign a fixed IP address to some device while using DHCP, you have to put this device's MAC address in the **Table of Fixed DHCP Host Entries**. There have ten fixed IP address location can use.
Every Ethernet device has a unique MAC(Media Access Control) address. The MAC address is assigned at factory and consists of six pairs of hexadecimal characters, for example, 00:03:79:0A:01:3F

Press Next to setup WAN1 parameters.

Some of the ISP provides DHCP server service by which the PC in LAN can access IP information automatically. To setup the DHCP client mode, follow the procedure

Set up IP address, Subnet Mask, Host Name with DHCP Client mode



BASIC - STEP2

LAN:

IP Type: ○ Fixed ● Dynamic(DHCP Client)

IP Address: 192 . 168 . 0 . 1

Subnet Mask: 255 . 255 . 255 . 0

Host Name: SOHO

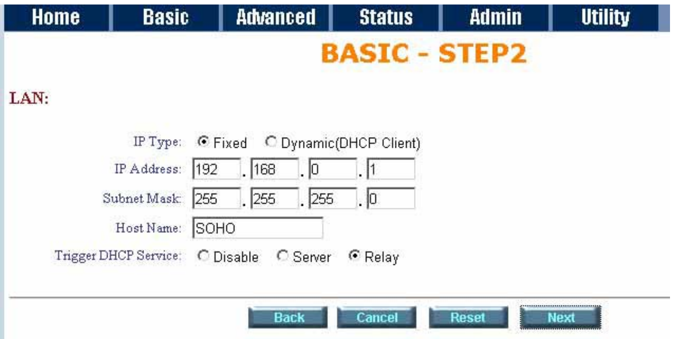
Trigger DHCP Service: ● Disable ○ Server ○ Relay

LAN IP Type: Dynamic(DHCP Client)

Click Next to setup WAN1 parameters.

DHCP relay

If you have a DHCP server in LAN and you want to use it for DHCP services, the product provides DHCP relay function to meet yours need.



BASIC - STEP2

LAN:

IP Type: ● Fixed ○ Dynamic(DHCP Client)

IP Address: 192 . 168 . 0 . 1

Subnet Mask: 255 . 255 . 255 . 0

Host Name: SOHO

Trigger DHCP Service: ○ Disable ○ Server ● Relay

IP Type: Fixed

IP Address: 192.168.0.1

Subnet Mask: 255.255.255.0

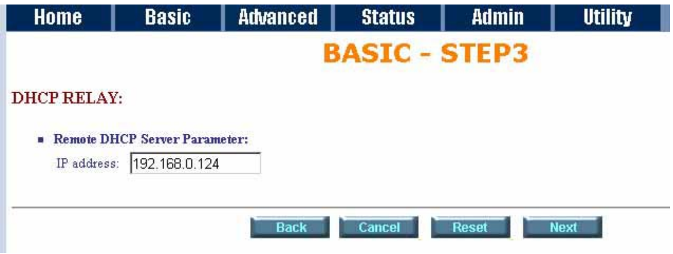
Host Name: SOHO

Some of the ISP requires the host name as identification. You may check with ISP to see if your Internet service has been configured with a host name. In most cases, this field can be ignored.

Trigger DHCP Service: Relay

Set up the DHCP Server

Press Next to setup **Remote DHCP server parameter**.



BASIC - STEP3

DHCP RELAY:

- **Remote DHCP Server Parameter:**

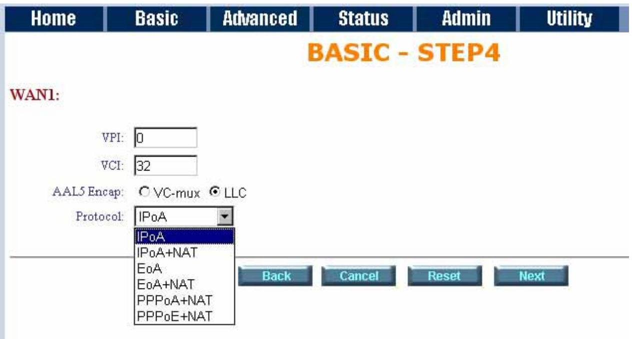
IP address: 192.168.0.124

If using DHCP relay service, there must set up the remote DHCP server IP address

Enter DHCP server IP address in IP address field.

Press Next

Set up the WAN1 VPI, VCI Encap. and Protocol



BASIC - STEP4

WAN1:

VPI: 0

VCI: 32

AAL5 Encap: ○ VC-mux ● LLC

Protocol: IPoA

VPI: 0

VCI: 33

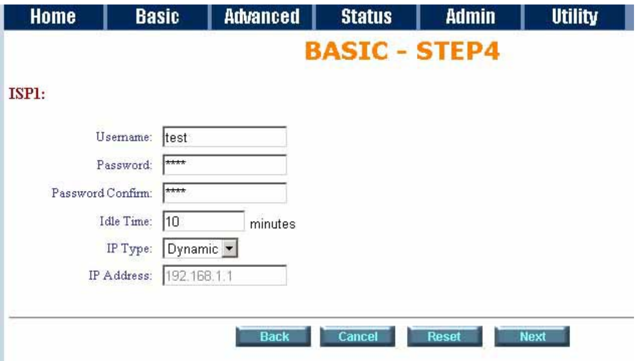
AAL5 Encap: LLC

Protocol: PPPoA + NAT or PPPoE + NAT

Click Next to setup User name and password.

For more understanding about NAT, review NAT/DMZ chapter.

If the Protocol using PPPoA+NAT or PPPoE+NAT, you must setup the ISP's parameters on the following:



BASIC - STEP4

ISP1:

Username: test

Password: ****

Password Confirm: ****

Idle Time: 10 minutes

IP Type: Dynamic

IP Address: 192.168.1.1

Type the ISP1 parameters.

Username: test

Password: test

Password Confirm: test

Your ISP will provide the user name and password.

Idle Time: 10

You want your Internet connection to remain on at all time, enter "0" in the Idle Time field.

IP Type: Dynamics.

The default IP type is Dynamic. It means that ISP PPP server will provide IP information including dynamic IP address when SHDSL.bis connection is established. On the other hand, you do not need to type the IP address of WAN1. Some of the ISP will provide fixed IP address over PPP. For fixed IP address:

IP Type: Fixed

IP Address: 192.168.1.1

Click Next.

Note: For safety, the password will be prompt as star symbol.

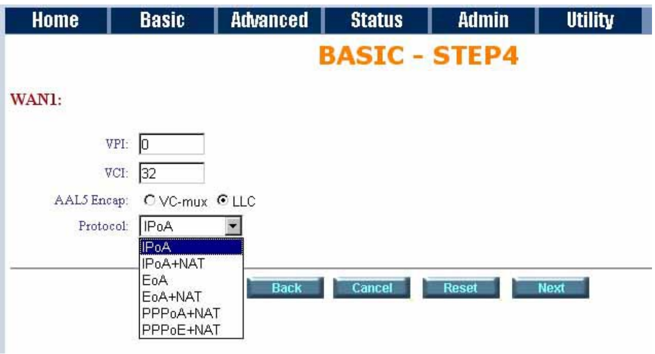
***Username** : Enter the user name exactly as your ISP assigned.*
***Password**: Enter the password associated with the user name above.*

***Password confirm**: Enter the password again for confirmation.*
***Idle Time**: When you don't want the connection up all the time and specify an idle time on this field.*
***IP type**: A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a differnet on each time you connect to the Internet.*

The screen will prompt the parameters that will be written in NVRAM. Check the parameters before writing in NVRAM.

Press Restart to restart the router working with new parameters or press to continue setting another parameter.

Set up : WAN1 VPI, VCI, Encap. and Protocol



BASIC - STEP4

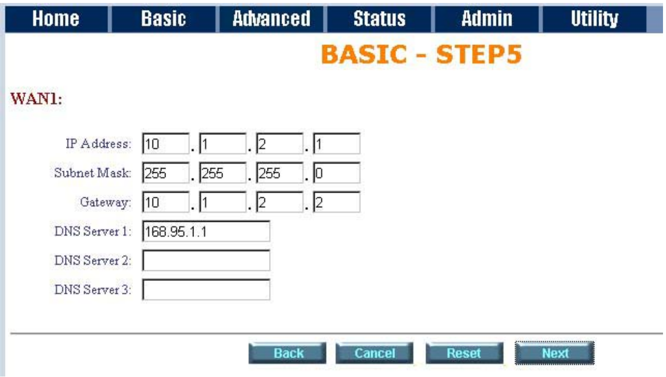
WAN1:

VPI: 0
VCI: 32
AAL5 Encap: ○ VC-mux ● LLC
Protocol: IPoA
IPoA
IPoA+NAT
EoA
EoA+NAT
PPPoA+NAT
PPPoE+NAT

WAN:
VPI: 0
VCI: 33
AAL5 Encap: LLC
Protocol: IPoA , EoA , IPoA + NAT or EoA + NAT
Click Next to setup the IP parameters.

For more understanding about NAT, review NAT/DMZ chapter.

Set up the WAN1 IP address, Subnet Mask, gateway and DNS Server



BASIC - STEP5

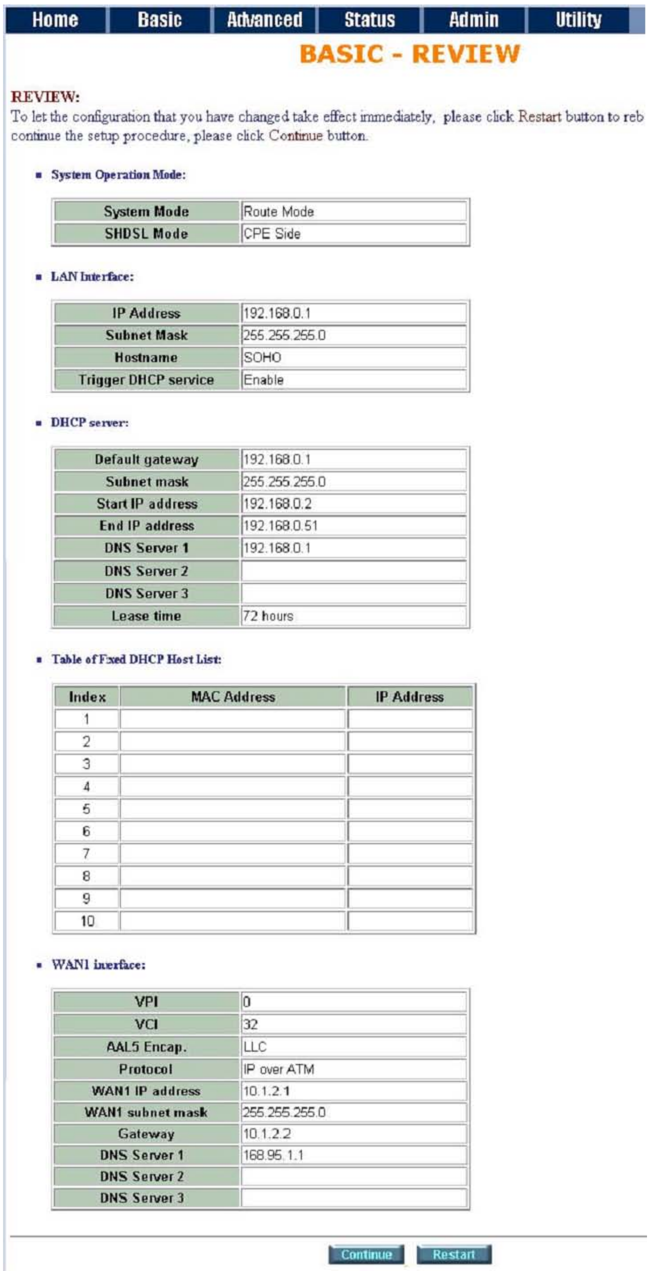
WAN1:

IP Address: 10 . 1 . 2 . 1
Subnet Mask: 255 . 255 . 255 . 0
Gateway: 10 . 1 . 2 . 2
DNS Server 1: 168.95.1.1
DNS Server 2:
DNS Server 3:

IP Address: 10.1.2.1
It is router IP address like from Internet. Your ISP will provide it and you need to specify here.
Subnet mask: 255.255.255.0
This is the router subnet mask seen by external users on Internet. Your ISP will provide it to you.
Gateway: 10.1.2.2
Your ISP will provide you the default gateway.
DNS Server 1: 168.95.1.1
Your ISP will provide at least one DNS (Domain Name System) Server IP address.

Click Next to review.

Review



BASIC - REVIEW

REVIEW:
To let the configuration that you have changed take effect immediately, please click Restart button to reb
continue the setup procedure, please click Continue button.

- System Operation Mode:

System Mode	Route Mode
SHDSL Mode	CPE Side

- LAN Interface:

IP Address	192.168.0.1
Subnet Mask	255.255.255.0
Hostname	SOHO
Trigger DHCP service	Enable

- DHCP server:

Default gateway	192.168.0.1
Subnet mask	255.255.255.0
Start IP address	192.168.0.2
End IP address	192.168.0.51
DNS Server 1	192.168.0.1
DNS Server 2	
DNS Server 3	
Lease time	72 hours

- Table of Fixed DHCP Host List:

Index	MAC Address	IP Address
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

- WAN1 inerface:

VPI	0
VCI	32
AAL5 Encap.	LLC
Protocol	IP over ATM
WAN1 IP address	10.1.2.1
WAN1 subnet mask	255.255.255.0
Gateway	10.1.2.2
DNS Server 1	168.95.1.1
DNS Server 2	
DNS Server 3	

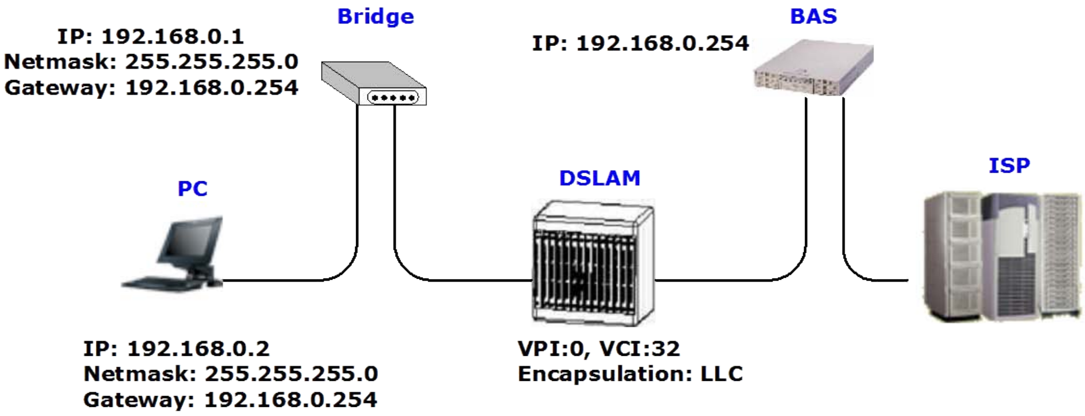
The screen will prompt the parameters that will be written in NVRAM. Check the parameters before writing in NVRAM.

Press Restart to restart the router working with new parameters or press **Continue** to setup another parameter.

4.1.3 Reference diagram

Bridge mode

When configured in Bridge Mode, the router will act as a pass-through device and allow the workstations on your LAN to have public addresses directly on the internet.

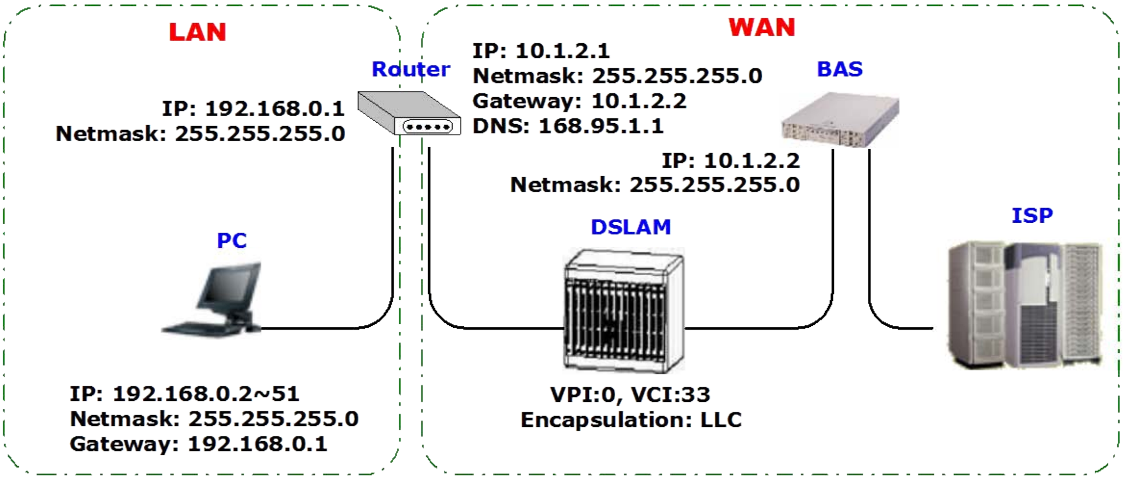


IPoA or EoA

IPoA (Dynamic IP over ATM) interfaces carries IP packets over AAL5. AAL5 provides the IP hosts on the same network with the data link layer for communications. In addition, to allow these hosts to communicate on the same ATM networks, IP packets must be tuned somewhat. AS the bearer network of IP services, ATM provides high speed point-to-point connections which considerably improve the bandwidth performance of IP network. On the other hand, ATM provides excellent network performance and perfect QoS.

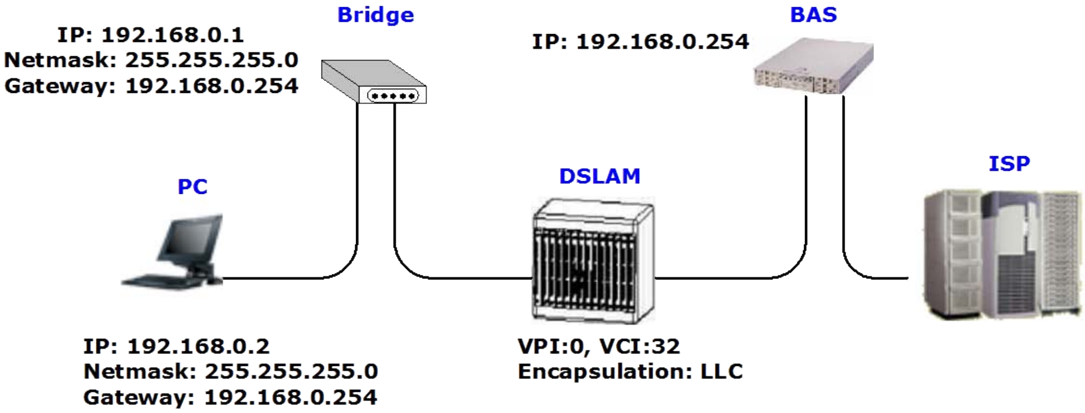
EoA (Ethernet-over-ATM) protocol is commonly used to carry data between local area networks that use the Ethernet protocol and wide-area networks that use the ATM protocol. Many telecommunications industry networks use the ATM protocol. ISPs who provide DSL services often use the EoA protocol for data transfer with their customers' DSL modems.

EoA can be implemented to provide a bridged connection between a DSL modem and the ISP. In a bridged connection, data is shared between the ISP's network and their customer's as if the networks were on the same physical LAN. Bridged connections do not use the IP protocol. EoA can also be configured to provide a routed connection with the ISP, which uses the IP protocol to exchange data.



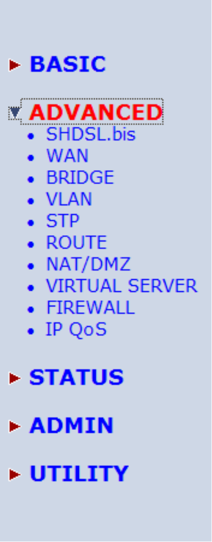
PPPoE or PPPoA

PPPoA (point-to-point protocol over ATM) and PPPoE (point-to-point protocol over Ethernet) are authentication and connection protocols used by many service providers for broadband Internet access. These are specifications for connecting multiple computer users on an Ethernet local area network to a remote site through common customer premises equipment, which is the telephone company's term for a modem and similar devices. PPPoE and PPPoA can be used to office or building. Users share a common Digital Subscriber Line (DSL), cable modem, or wireless connection to the Internet. PPPoE and PPPoA combine the Point-to-Point Protocol (PPP), commonly used in dialup connections, with the Ethernet protocol or ATM protocol, which supports multiple users in a local area network. The PPP protocol information is encapsulated within an Ethernet frame or ATM frame.



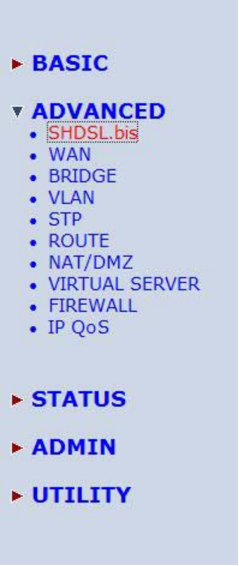
4.2 Advanced Setup

Advanced setup contains **SHDSL.bis, WAN, Bridge, VLAN, Ethernet, Route, NAT/DMZ, Virtual SERVER, FIREWALL and IP QoS** parameters.

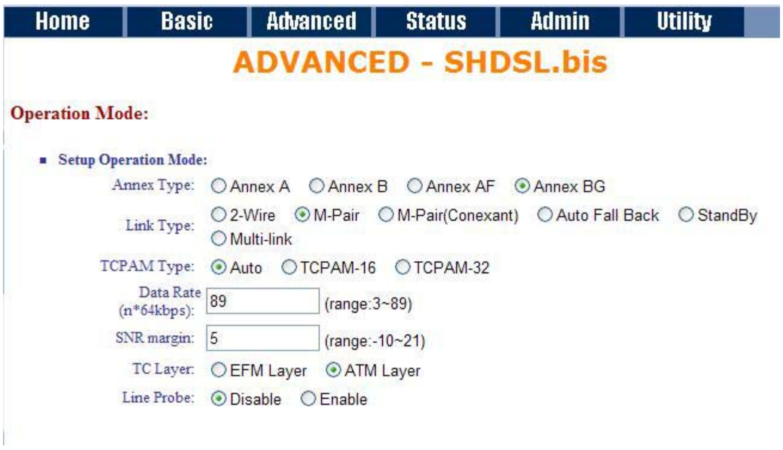


4.2.1 SHDSL.bis

You can setup the Annex type, data rate and SNR margin for SHDSL.bis parameters in UM-SB. Click UM-SB



Enter Parameters in UM-SB



ADVANCED - SHDSL.bis

Operation Mode:

- Setup Operation Mode:

Annex Type:	○ Annex A ○ Annex B ○ Annex AF ● Annex BG
Link Type:	○ 2-Wire ● M-Pair ○ M-Pair(Conexant) ○ Auto Fall Back ○ StandBy ○ Multi-link
TCPAM Type:	● Auto ○ TCPAM-16 ○ TCPAM-32
Data Rate (n*64kbps):	89 (range:3~89)
SNR margin:	5 (range:-10~21)
TC Layer:	○ EFM Layer ● ATM Layer
Line Probe:	● Disable ○ Enable

4.2.1.1 Annex Type

There are four Annex types: **Annex A** (ANSI), **Annex B** (ETSI), **AnnexAF** and **Annex BG** . It the router must connect to your ISP, please check them about it. If your routers configed to point to point application, you must choose one of the four types according to which line rate you need.

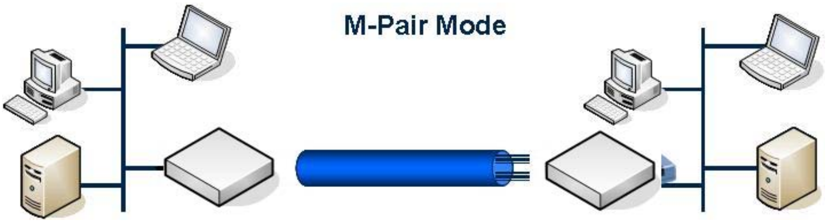
4.2.1.2 Line Type

There are six type of line type for you choose: **2-wire**, **M-Pair**, **M-Pair(Conexant)**, **Auto Fall Back**, **StandBy** and **Multi-link.**

2-wire mode

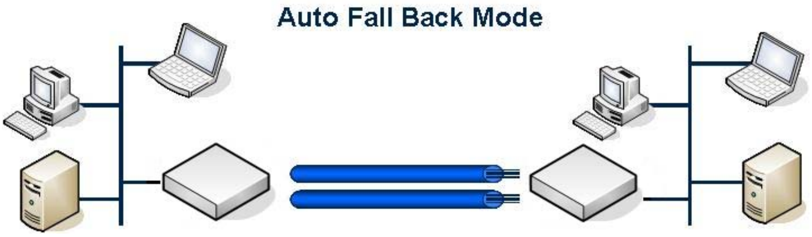
For 4-wires model, it can use only the first one pair for the single pair DSL wire application.

M – Pair Mode



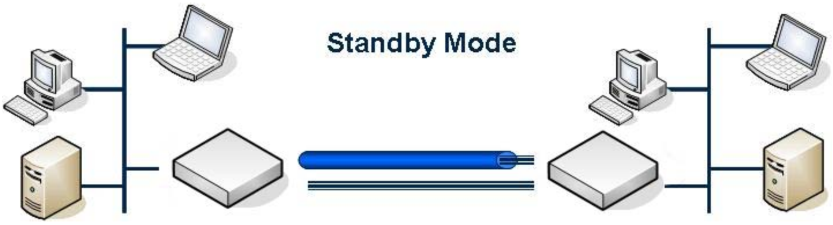
In this mode, each wire pairs of Dynamix UM-SB router must be configured with the same line rate. If one pair fails then the entire line must be restarted. It also has the Conexant M-pair standard used with connection to other router with Conexant chip set solution.

Auto Fall Back Mode



Two DSL pairs are working simultaneously. When one pair of both is disconnect, the other pair will keep working.

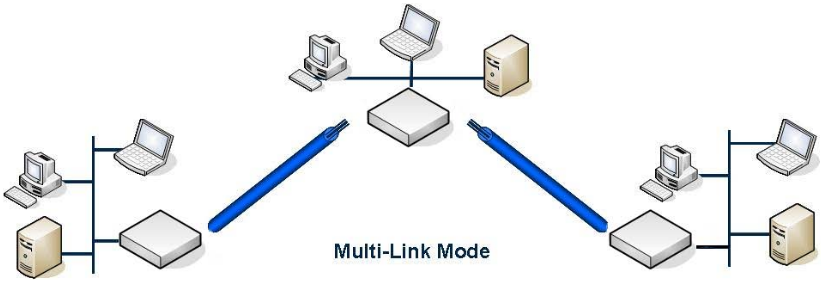
Stanby Mode



Only one of two pairs are working, other pair is standby. If the working pair fails, the standby pair will start up to continues.

Multi–Link Mode

For 4-wires model, each pair will connect to two different remote device, which may or may not be in the same location. Channel A used as CO side and Channel B used as CPE side.



4.2.1.3 TCPAM Type

TCPAM stands for Trellis Coded Pulse Amplitude Modulation. It is the modulation format that is used in both HDSL2 and SHDSL, and provides robust performance over a variety of loop conditions. SHDSL.bis supports 16 level TCPAM line code(TPCAM-16) or 32 level TCPAM line code(TCPAM-32) to provide a rate/reach adaptive capability, offering enhanced performance (increased rate or reach) and improved spectral compatibility. The default option is Auto. You may assign the different type manually by click the caption TPCAM-16 or TPCAM-32. Only Annex AF and BG can using TCPAM-32.

4.2.1.4 Data Rate

For 2-wire model **(n*64kbps)**

You can setup the SHDSL.bis data rate in the multiple of 64kbps.

The default data rate is 5696Kbps (n=89).

For using Annex AF or BG

TCPAM32 ; data rate is 768Kbps ~ 5696Kbps (Nx64kbps, N=12~89)

TCPAM16 ; data rate is 192Kbps ~ 3840Kbps (Nx64kbps, N=3~60)

For uning Annex A or B

TCPAM16 ; 192Kbps ~ 2304Kbps (Nx64kbps, N=3~36)

For 4-wire model **(n*128kbps)**

You can setup the SHDSL.bis data rate in the multiple of 128kbps.

The default data rate is 11392Kbps (n=89).

For using Annex AF or BG

TCPAM32 ; data rate is 1536Kbps ~ 11392Kbps (Nx128kbps, N=12~ 89)

TCPAM16 ; data rate is 384Kbps ~ 7680Kbps (Nx128kbps, N=3~60)
For using Annex A or B
TCPAM16 ; 384Kbps ~ 4608Kbps (Nx128kbps, N=3~36)

		2-wire model	4-wire model
Annex A/B	TCPAM-16	192~2304 kbps	384~4608 kbps
Annex AF/BG	TCPAM-16	192~3840 kpbs	384~7680 kbps
	TCPAM-32	768~5696 kpbs	1536~11392 kbps

4.2.1.5 SNR Margin

This is an index of line connection quality. You can see the actual SNR margin in STATUS SHDSL.bis. The larger is SNR margin, the better is line connection quality.
The range of SNR Margin is -10 to 21.

If you set SNR margin in the field as 3, the SHDSL.bis connection will drop and reconnect when the SNR margin is lower than 3. On the other hand, the device will reduce the line rate and reconnect for better line connection quality.

4.2.1.6 TC Layer

There have two TC layer setting on this router: EFM layer and ATM layer. According which networks connected: ATM based access networks or Ethernet based access networks

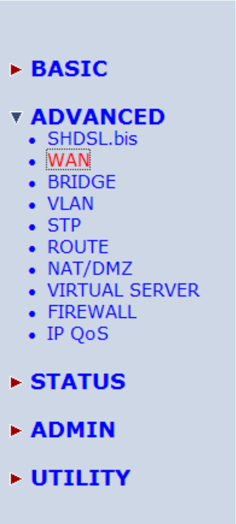
4.2.1.7 Line Probe

For adaptive mode, you have to Enable this Line Probe. The router will adapt the data rate according to the line status.

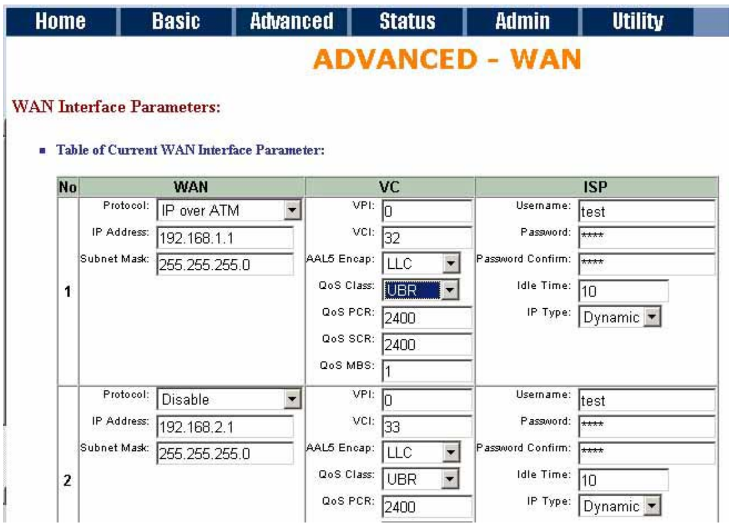
The screen will prompt the parameters that will be written in NVRAM. Check the parameters before writing in NVRAM.
Press Restart to restart the router working with new parameters or press continue to setup another parameter.

4.2.2 WAN

The router can support up to 8 PVCs. WAN 1 was configured via **BASIC** menu except QoS. If you want to setup another PVCs such as WAN 2 to 7, those parameters are setup on the pages of WAN under ADVANCED. On the other hand, you don't need to setup WAN except you apply two or more Internet Services with ISPs.



The parameters in WAN Number 1 has been setup in Basic Setup.
If you want to setup another PVC, you can configure in WAN 2 to WAN 8.



ADVANCED - WAN

WAN Interface Parameters:

- Table of Current WAN Interface Parameter:

No	WAN	VC	ISP
1	Protocol: IP over ATM IP Address: 192.168.1.1 Subnet Mask: 255.255.255.0	VPI: 0 VCI: 32 AAL5 Encap: LLC QoS Class: UBR QoS PCR: 2400 QoS SCR: 2400 QoS MBS: 1	Username: test Password: **** Password Confirm: **** Idle Time: 10 IP Type: Dynamic
2	Protocol: Disable IP Address: 192.168.2.1 Subnet Mask: 255.255.255.0	VPI: 0 VCI: 33 AAL5 Encap: LLC QoS Class: UBR QoS PCR: 2400	Username: test Password: **** Password Confirm: **** Idle Time: 10 IP Type: Dynamic

Enter the parameters:

Protocol: If WAN Protocol is PPPoA or PPPoE with dynamic IP, leave the default WAN IP Address and Subnet Mask as default setting. The system will ingore the IP Address and Subnet Mask information, but erasion or blank in default setting will cause system error.

If the WAN Protocol is IPoA or EoA, leave the ISP parameters as default setting. The system will ingore the information, but erasion or blank in default setting will cause system error.

VC-mux (VC-based Multiplexing): Each protocol is assigned to a specific virtual circuit. VC-based multiplexing may be dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical.

LLC (LLC-based Multiplexing): One VC carries multiptle protocols with protocol identifying information being contained in each packet header. Deapite the extra bandwidth and processing overhead, this method may be advantagrous if it is not practical to have a sepatate VC for each carried protocol.

VPI (Virtual Path Identifier) is for set up ATM Permanent Virtual Channels(PVC).The valid range for

VPI is 0 to 255.

VCI (Virtual Channel Identifier is for set up ATM Permanent Virtual Channels(PVC). The valid range for VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic.)

QoS (Quality of Service) **class** : The Traffic Management Specification V4.0 defines ATM service cataloges that describe both the traffic transmitted by users onto a network as well as the Quailty of Service that the network need to provide for that traffic. There have four class four choice: UBR, CBR, rt-VBR and nrt-VBR. Select CBR to specify fixed bandwidth for voice or data traffic. Select UBR for applications that are non-time sensitive, such as e-mail. Slect VBR for bursty traffic and bandwidth sharing with other applications.

UBR (Unspecified Bit Rate) is the simplest service provided by ATM networks. There is no guarantee of anything. It is a primary service used for transferring Internet traffic over the ATM network.

CBR (Constant Bit Rate) is used by connections that requires a static amount of bandwidth that is avilable during the connection life time. This bandwidth is characterized by Peak Cell Rate (PCR). Based on the PCR of the CBR traffic, specific cell slots are assigned for the VC in the schedule table. The ATM always sends a signle cell during the CBR connection's assigned cell slot.

VBR-rt (Varible Bit Rate real-time) is intended for real-time applications, such as compressed voice over IP and video comferencing, that require tightly constrained delays and delay variation. VBR-rt is characterized by a peak cell rate (PCR), substained cell rate (SCR), and maximun burst rate (MBR).

VBR-nrt (Varible Bit Rate non-real-time) i*s intended for non-real-time applications, such as FTP, e-mail and browsing.*

PCR (Peak Cell Rate) in kbps: The maximum rate at which you expect to transmit data, voice and video. Consider PCR and MBS as a menas of reducing lantency, not increasing bandwidth. The range of PCR is 384kbps to 11392kbps

SCR (Substained Cell Rate): The sustained rate at which you expect to transmit data, voice and video. Consider SCR to be the true bandwidth of a VC and not the lone-term average traffic rate. The range of SCR is 384kbps to 11392kbps.

MBS (Maximum Burst Size): Refers to the maximum number of cells that can be sent at the peak rate. The range of MBS is 1 cell to 255 cells.

Username : Enter the user name exactly as your ISP assigned.

Password: Enter the password associated with the user name above.

Password confirm: Enter the password again for confirmation.

Idle Time: When you don't want the connection up all the time and specify an idle time on this field.

IP type: A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a differnet on each time you connect to the Internet.

Press Finish to finish setting.

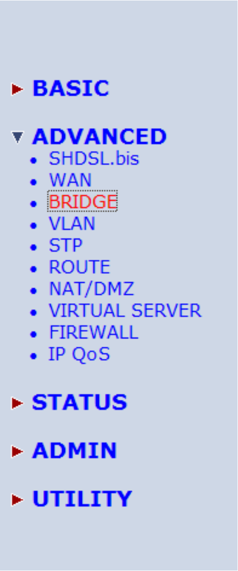
The screen will prompt the parameters that will be written in NVRAM. Check the parameters before writing in NVRAM.

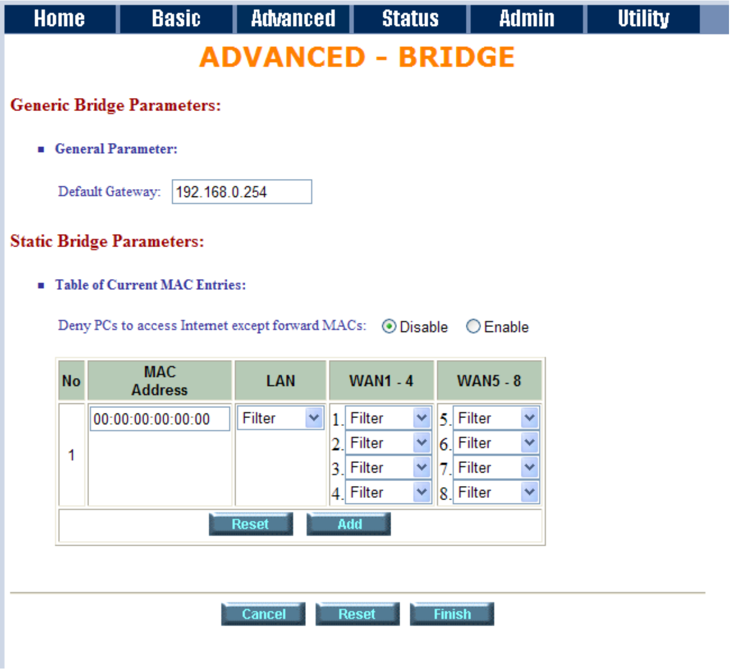
Press Restart to restart the router working with new parameters or press continue to setup another parameter.

4.2.3 Bridge

If you want to setup advanced filter function while router is working in bridge mode, you can use **BRIDGE** menu to setup the filter function, blocking function.

Click Bridge to setup.





ADVANCED - BRIDGE

Generic Bridge Parameters:

- General Parameter:

Default Gateway: 192.168.0.254

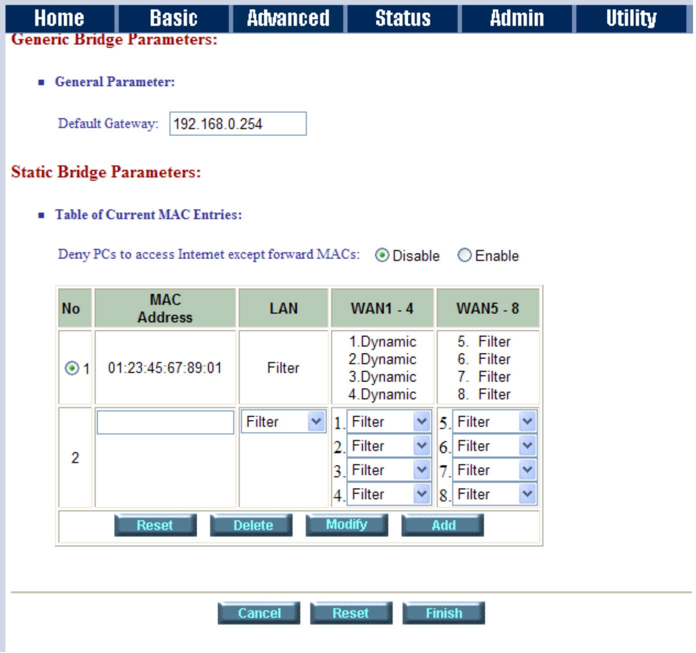
Static Bridge Parameters:

- Table of Current MAC Entries:

Deny PCs to access Internet except forward MACs: ● Disable ○ Enable

No	MAC Address	LAN	WAN1 - 4	WAN5 - 8
1	00:00:00:00:00:00	Filter	1. Filter 2. Filter 3. Filter 4. Filter	5. Filter 6. Filter 7. Filter 8. Filter

Press Add in the bottom of web page to add the static bridge information.



Generic Bridge Parameters:

- General Parameter:

Default Gateway: 192.168.0.254

Static Bridge Parameters:

- Table of Current MAC Entries:

Deny PCs to access Internet except forward MACs: ● Disable ○ Enable

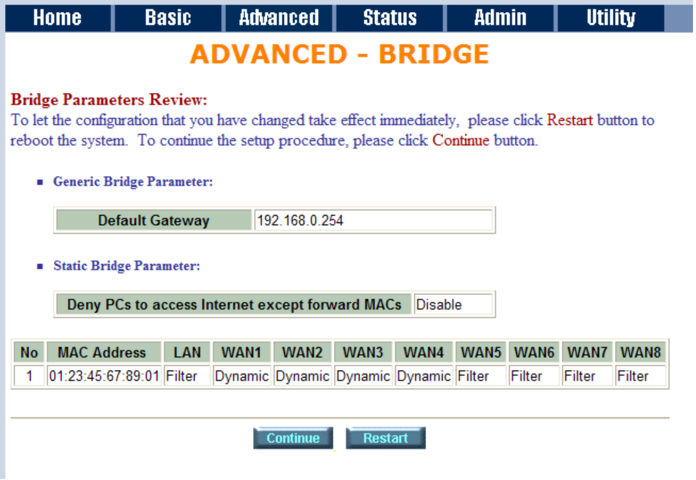
No	MAC Address	LAN	WAN1 - 4	WAN5 - 8
● 1	01:23:45:67:89:01	Filter	1.Dynamic 2.Dynamic 3.Dynamic 4.Dynamic	5. Filter 6. Filter 7. Filter 8. Filter
2		Filter	1. Filter 2. Filter 3. Filter 4. Filter	5. Filter 6. Filter 7. Filter 8. Filter

If you want to filter the designated MAC address of LAN PC to access Internet, press Add to establish the filtering table. Put the MAC address in **MAC Address** field and select Filter in **LAN** field.

If you want to filter the designated MAC address of WAN PC to access LAN, press Add to establish the filtering table. Key the MAC address in **MAC Address** field and select Filter in WAN field.

For example: if your VC is setup at WAN 1, select WAN 1 Filter.

Press Finish in the bottom of web page to review the bridge parameters.



ADVANCED - BRIDGE

Bridge Parameters Review:
To let the configuration that you have changed take effect immediately, please click Restart button to reboot the system. To continue the setup procedure, please click Continue button.

- Generic Bridge Parameter:

Default Gateway	192.168.0.254

- Static Bridge Parameter:

Deny PCs to access Internet except forward MACs	Disable

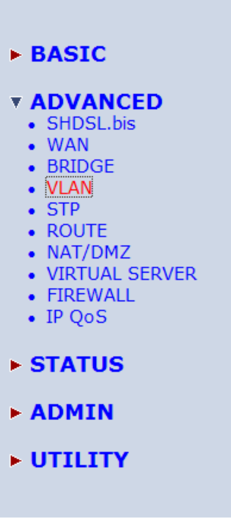
No	MAC Address	LAN	WAN1	WAN2	WAN3	WAN4	WAN5	WAN6	WAN7	WAN8
1	01:23:45:67:89:01	Filter	Dynamic	Dynamic	Dynamic	Dynamic	Filter	Filter	Filter	Filter

The screen will prompt the parameters that will be written in NVRAM. Check the parameters before writing in NVRAM.

Press Restart to restart the router working with new parameters or press Continue to setup another parameter.

4.2.4 VLAN

Click VLAN to configure VLAN.

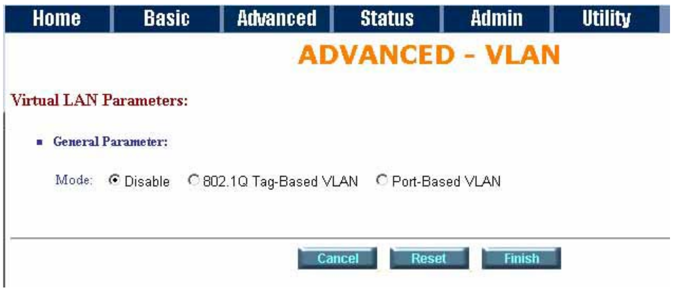


VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group.

With MTU (Multi-Tenant Unit) applications, VLAN is vital in providing isolation and security among the subscribers. When properly configured, VLAN prevents one subscriber from accessing the network resources of another on the same LAN.

VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

The IEEE 802.1Q defines the operation of VLAN bridges that permit the definition, operation, and administration of VLAN topologies within a bridged LAN infrastructure.

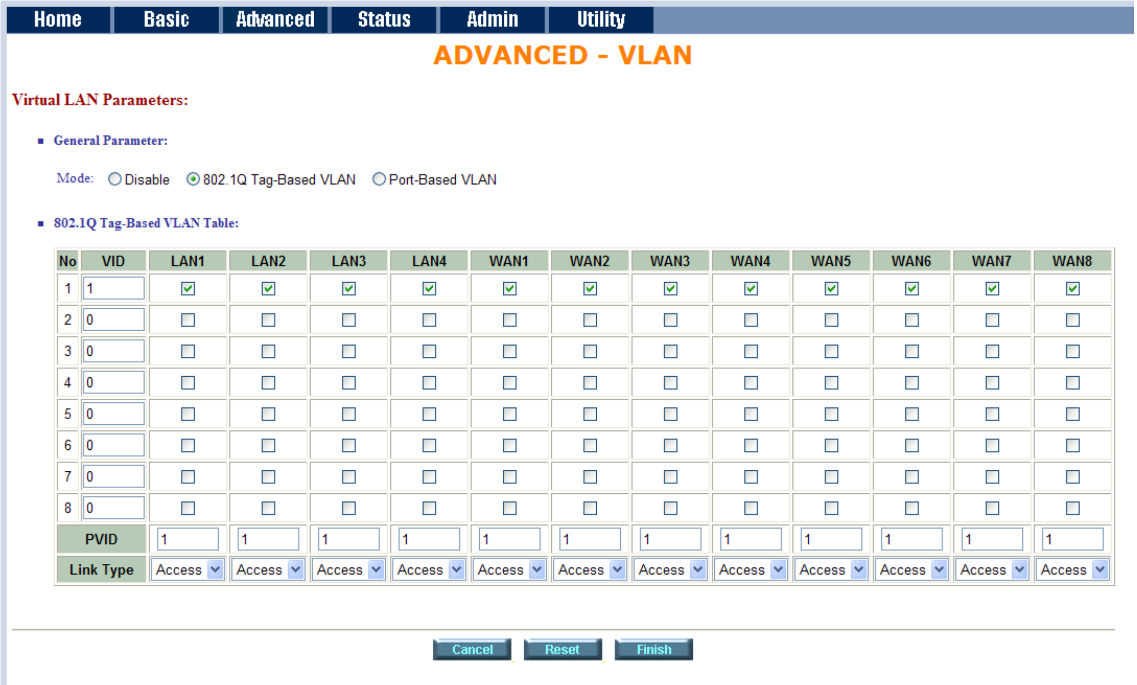


Mode: ● Disable ○ 802.1Q Tag-Based VLAN ○ Port-Based VLAN

The router supports two types of VLAN: **802.1Q Tag-Based VLAN** and **Port-Based VLAN**. User can configure one of them to the router.

4.2.4.1 802.1Q Tag-Based VLAN

For setting 802.1Q VLAN click the 802.1Q Tagt-Based VLAN. The screem will prompt as following.



ADVANCED - VLAN

Virtual LAN Parameters:

- General Parameter:

Mode: ○ Disable ● 802.1Q Tag-Based VLAN ○ Port-Based VLAN

- 802.1Q Tag-Based VLAN Table:

No	VID	LAN1	LAN2	LAN3	LAN4	WAN1	WAN2	WAN3	WAN4	WAN5	WAN6	WAN7	WAN8
1	1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
2	0	□	□	□	□	□	□	□	□	□	□	□	□
3	0	□	□	□	□	□	□	□	□	□	□	□	□
4	0	□	□	□	□	□	□	□	□	□	□	□	□
5	0	□	□	□	□	□	□	□	□	□	□	□	□
6	0	□	□	□	□	□	□	□	□	□	□	□	□
7	0	□	□	□	□	□	□	□	□	□	□	□	□
8	0	□	□	□	□	□	□	□	□	□	□	□	□
PVID		1	1	1	1	1	1	1	1	1	1	1	1
Link Type		Access	Access	Access	Access	Access	Access	Access	Access	Access	Access	Access	Access

VID: (Virtual LAN ID) It is an definite number of ID which number is from 1 to 4094.
PVID: (Port VID) It is an untagged member from 1 to 4094 of default VLAN.
Link Type: Access means the port can receive or send untagged packets.
Trunk means that the prot can receive or send tagged packets.

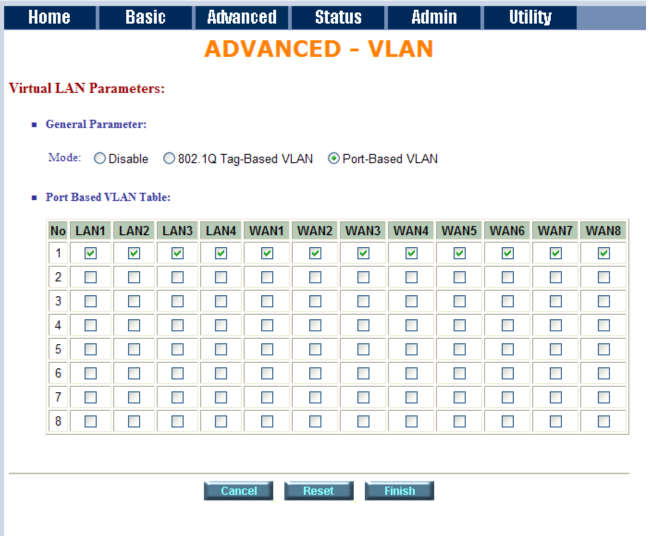
The router initially default configures one VLAN, VID=1.
A port such as LAN1 to LAN4 and WAN1 to WAN8 can have only one PVID, but can have as many VID as the router has memory in its VLAN table to store them.

Ports in the same VLAN group share the same frame broadcast domin thus increase network performance through reduced boardcast traffic. VLAN groups can be modified at any time by adding, moving or changing ports without any re-cabling.

4.2.4.2 Port-Based VLAN

Port-Based VLANs are VLANs where the packet forwarding decision is based on the destination MAC address and its associated port.

For setting Port-Based VLAN, Click Port-Based VLAN, The screem will prompt as following:



ADVANCED - VLAN

Virtual LAN Parameters:

- General Parameter:

Mode: ○ Disable ○ 802.1Q Tag-Based VLAN ● Port-Based VLAN

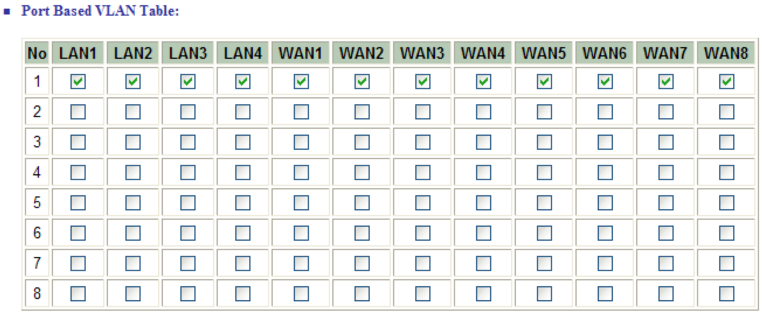
- Port Based VLAN Table:

No	LAN1	LAN2	LAN3	LAN4	WAN1	WAN2	WAN3	WAN4	WAN5	WAN6	WAN7	WAN8
1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
2	□	□	□	□	□	□	□	□	□	□	□	□
3	□	□	□	□	□	□	□	□	□	□	□	□
4	□	□	□	□	□	□	□	□	□	□	□	□
5	□	□	□	□	□	□	□	□	□	□	□	□
6	□	□	□	□	□	□	□	□	□	□	□	□
7	□	□	□	□	□	□	□	□	□	□	□	□
8	□	□	□	□	□	□	□	□	□	□	□	□

Port-Based VLANs are VLANs where the packet forwarding decision is based on the destination MAC address and its associated port.

When using the port-based VLAN, the port is assigned to a specific VLAN independent of the user or system attached to the port. This means all users attached to the port should be members in the same VLAN. The network administrator typically performs the VLAN assignment. The port configuration is static and cannot be automatically changed to another VLAN without manual reconfiguration.

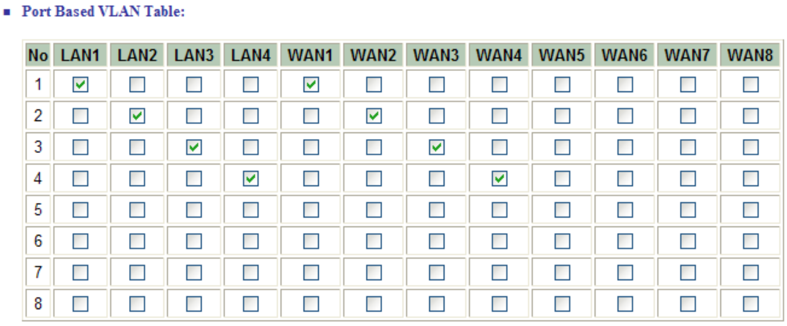
As with other VLAN approaches, the packets forwarded using this method do not leak into other VLAN domains on the network. After a port has been assigned to a VLAN, the port cannot send to or receive from devices in another VLAN.



- Port Based VLAN Table:

No	LAN1	LAN2	LAN3	LAN4	WAN1	WAN2	WAN3	WAN4	WAN5	WAN6	WAN7	WAN8
1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
2	□	□	□	□	□	□	□	□	□	□	□	□
3	□	□	□	□	□	□	□	□	□	□	□	□
4	□	□	□	□	□	□	□	□	□	□	□	□
5	□	□	□	□	□	□	□	□	□	□	□	□
6	□	□	□	□	□	□	□	□	□	□	□	□
7	□	□	□	□	□	□	□	□	□	□	□	□
8	□	□	□	□	□	□	□	□	□	□	□	□

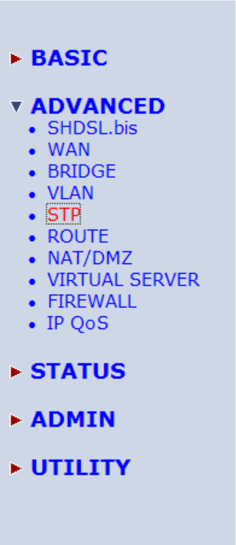
The default setting is all ports (LAN1 to LAN4 and WAN1 to WAN8) connected together which means all ports can communicate with each other. That is, there are no virtual LANs. The option is the most flexible but the least secure.



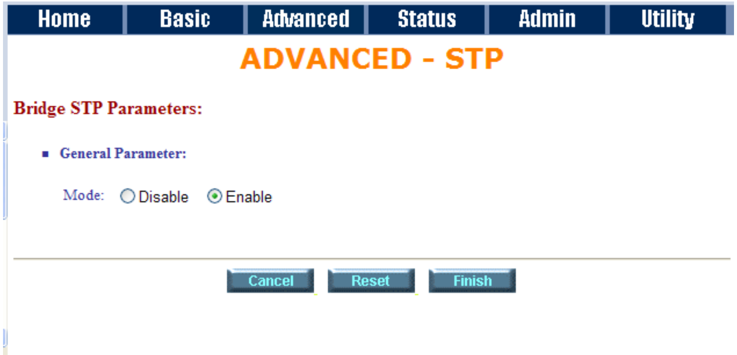
- Port Based VLAN Table:

No	LAN1	LAN2	LAN3	LAN4	WAN1	WAN2	WAN3	WAN4	WAN5	WAN6	WAN7	WAN8
1	☑	□	□	□	☑	□	□	□	□	□	□	□
2	□	☑	□	□	□	☑	□	□	□	□	□	□
3	□	□	☑	□	□	□	☑	□	□	□	□	□
4	□	□	□	☑	□	□	□	☑	□	□	□	□
5	□	□	□	□	□	□	□	□	□	□	□	□
6	□	□	□	□	□	□	□	□	□	□	□	□
7	□	□	□	□	□	□	□	□	□	□	□	□
8	□	□	□	□	□	□	□	□	□	□	□	□

4.2.5 STP



Click STP can disable or enable the bridge STP mode.



ADVANCED - STP

Bridge STP Parameters:

- General Parameter:

Mode: ○ Disable ● Enable

STP (Spanning-Tree Protocol) defined in the IEEE 802.1D, is a link management protocol that provides path redundancy while preventing undesirable loops in the network. For an Ethernet network to function properly, only one active path can exist between two stations.

Multiple active paths between stations cause loops in the network. If a loop exists in the network topology, the potential exists for duplication of messages. When loops occur, some switches see stations appear on both sides of the switch. This condition confuses the forwarding algorithm and allows duplicate frames to be forwarded.

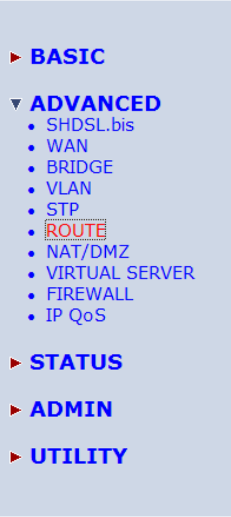
To provide path redundancy, Spanning-Tree Protocol defines a tree that spans all switches in an extended network. Spanning-Tree Protocol forces certain redundant data paths into a standby (blocked) state. If one network segment in the Spanning-Tree Protocol becomes unreachable, or if Spanning-Tree Protocol costs change, the spanning-tree algorithm reconfigures the spanning-tree topology and reestablishes the link by activating the standby path.

Spanning-Tree Protocol operation is transparent to end stations, which are unaware whether they are connected to a single LAN segment or a switched LAN of multiple segments.

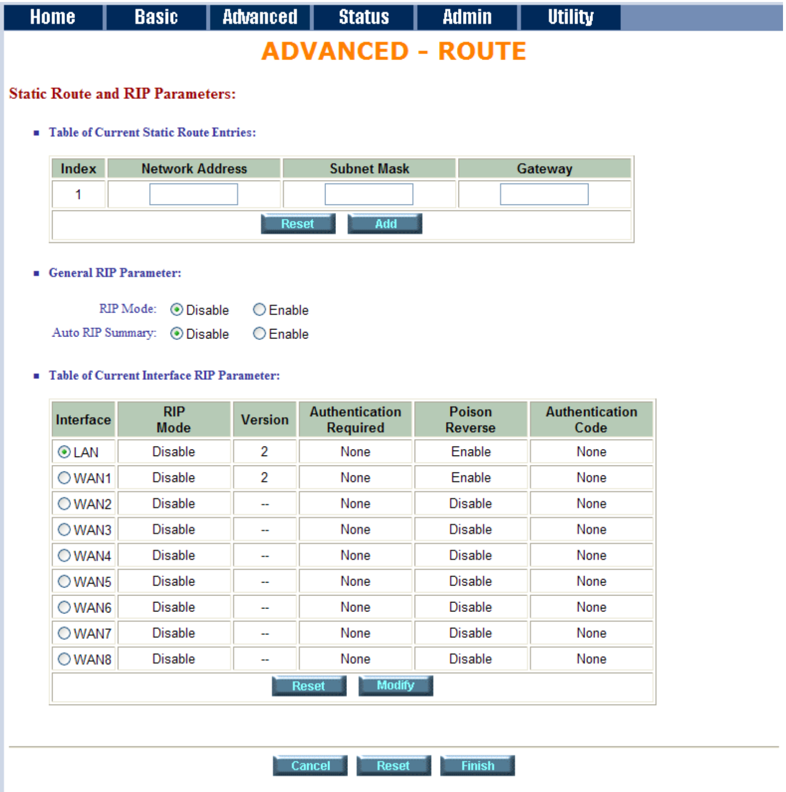
4.2.6 Route

If the Router is connected to more than one network, it may be necessary to set up a static route between them. A static route is a pre-determined pathway that network information must travel to reach a specific host or network.

With Dynamic Routing, you can enable the Router to automatically adjust to physical changes in the network's layout. The Router, using the RIP protocol, determines the network packets' route based on the fewest number of hops between the source and the destination. The RIP protocol regularly broadcasts routing information to other routers on the network.



Click Route to modify the routing information.



ADVANCED - ROUTE

Static Route and RIP Parameters:

- Table of Current Static Route Entries:

Index	Network Address	Subnet Mask	Gateway
1			

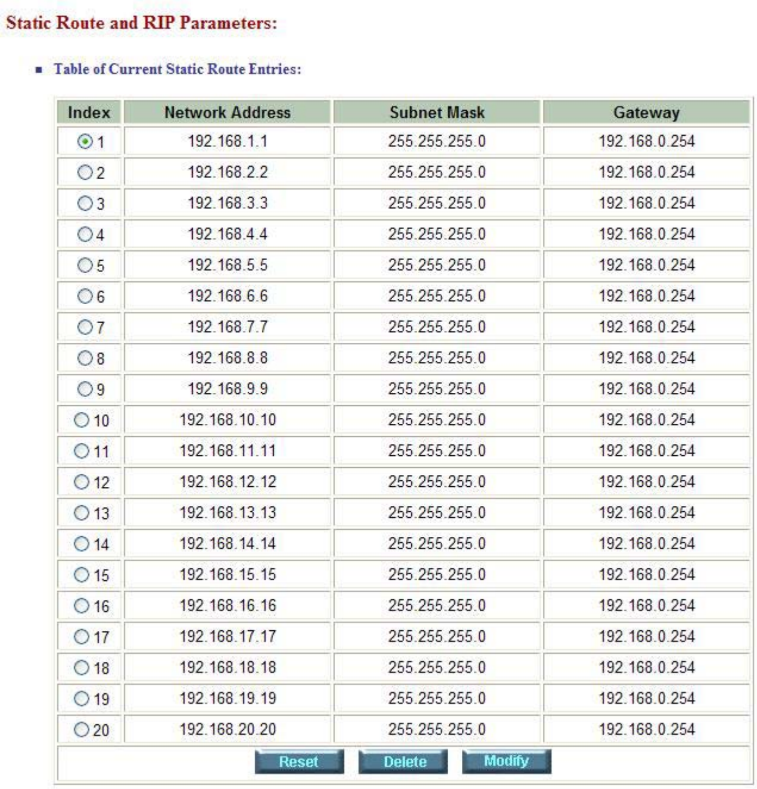
- General RIP Parameter:

RIP Mode: ● Disable ○ Enable
Auto RIP Summary: ● Disable ○ Enable

- Table of Current Interface RIP Parameter:

Interface	RIP Mode	Version	Authentication Required	Poison Reverse	Authentication Code
● LAN	Disable	2	None	Enable	None
○ WAN1	Disable	2	None	Enable	None
○ WAN2	Disable	--	None	Disable	None
○ WAN3	Disable	--	None	Disable	None
○ WAN4	Disable	--	None	Disable	None
○ WAN5	Disable	--	None	Disable	None
○ WAN6	Disable	--	None	Disable	None
○ WAN7	Disable	--	None	Disable	None
○ WAN8	Disable	--	None	Disable	None

There have maximun 20 entries to set up the static router.
Press Add to add each entry. For example, there are 20 entries of the following:

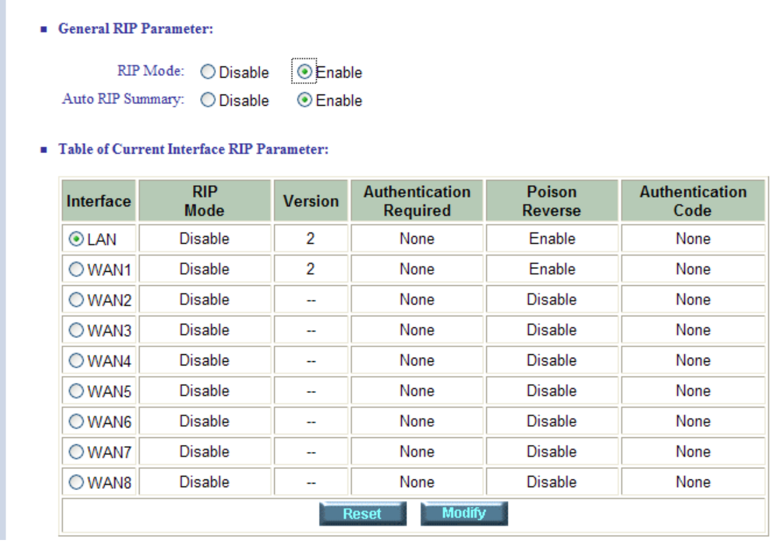


Static Route and RIP Parameters:

- Table of Current Static Route Entries:

Index	Network Address	Subnet Mask	Gateway
● 1	192.168.1.1	255.255.255.0	192.168.0.254
○ 2	192.168.2.2	255.255.255.0	192.168.0.254
○ 3	192.168.3.3	255.255.255.0	192.168.0.254
○ 4	192.168.4.4	255.255.255.0	192.168.0.254
○ 5	192.168.5.5	255.255.255.0	192.168.0.254
○ 6	192.168.6.6	255.255.255.0	192.168.0.254
○ 7	192.168.7.7	255.255.255.0	192.168.0.254
○ 8	192.168.8.8	255.255.255.0	192.168.0.254
○ 9	192.168.9.9	255.255.255.0	192.168.0.254
○ 10	192.168.10.10	255.255.255.0	192.168.0.254
○ 11	192.168.11.11	255.255.255.0	192.168.0.254
○ 12	192.168.12.12	255.255.255.0	192.168.0.254
○ 13	192.168.13.13	255.255.255.0	192.168.0.254
○ 14	192.168.14.14	255.255.255.0	192.168.0.254
○ 15	192.168.15.15	255.255.255.0	192.168.0.254
○ 16	192.168.16.16	255.255.255.0	192.168.0.254
○ 17	192.168.17.17	255.255.255.0	192.168.0.254
○ 18	192.168.18.18	255.255.255.0	192.168.0.254
○ 19	192.168.19.19	255.255.255.0	192.168.0.254
○ 20	192.168.20.20	255.255.255.0	192.168.0.254

To modify the RIP (Routing information protocol) Parameters:
RIP Mode: Enable
Auto RIP Summary: Enable
Press Modify



- General RIP Parameter:

RIP Mode: ○ Disable ● Enable
Auto RIP Summary: ○ Disable ● Enable

- Table of Current Interface RIP Parameter:

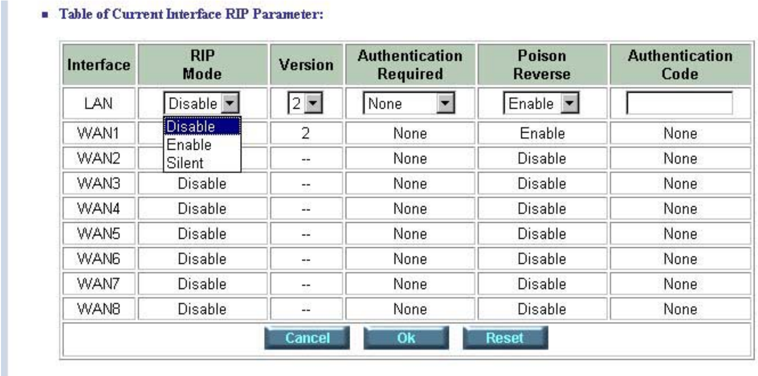
Interface	RIP Mode	Version	Authentication Required	Poison Reverse	Authentication Code
● LAN	Disable	2	None	Enable	None
○ WAN1	Disable	2	None	Enable	None
○ WAN2	Disable	--	None	Disable	None
○ WAN3	Disable	--	None	Disable	None
○ WAN4	Disable	--	None	Disable	None
○ WAN5	Disable	--	None	Disable	None
○ WAN6	Disable	--	None	Disable	None
○ WAN7	Disable	--	None	Disable	None
○ WAN8	Disable	--	None	Disable	None

RIP Mode:
This parameter determines how the router handle RIP (Routing information protocol). RIP allows it to exchange routing information with other router.

Disable: The gateway does not participate in any RIP exchange with other router.

Enable: The router broadcasts the routing table of the router on the LAN and incoporates RIP broadcast by other routers into it's routing table.

Silent: The router does not broadcast the routing table, but it accepts RIP broadcast packets that it receives.



▪ Table of Current Interface RIP Parameter:

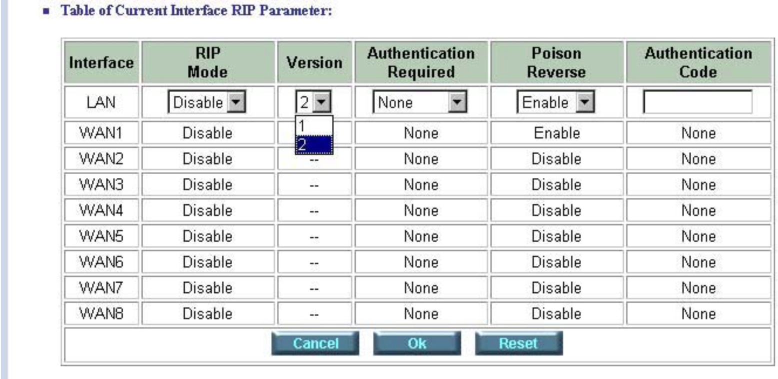
Interface	RIP Mode	Version	Authentication Required	Poison Reverse	Authentication Code
LAN	Disable	2	None	Enable	
WAN1		2	None	Enable	None
WAN2		--	None	Disable	None
WAN3	Disable	--	None	Disable	None
WAN4	Disable	--	None	Disable	None
WAN5	Disable	--	None	Disable	None
WAN6	Disable	--	None	Disable	None
WAN7	Disable	--	None	Disable	None
WAN8	Disable	--	None	Disable	None

RIP Version:

It determines the format and broadcasting method of any RIP transmissions by the gateway.

RIP v1: it only sends RIP v1 messages only.

RIP v2: it send RIP v2 messages in multicast and broadcast format.



▪ Table of Current Interface RIP Parameter:

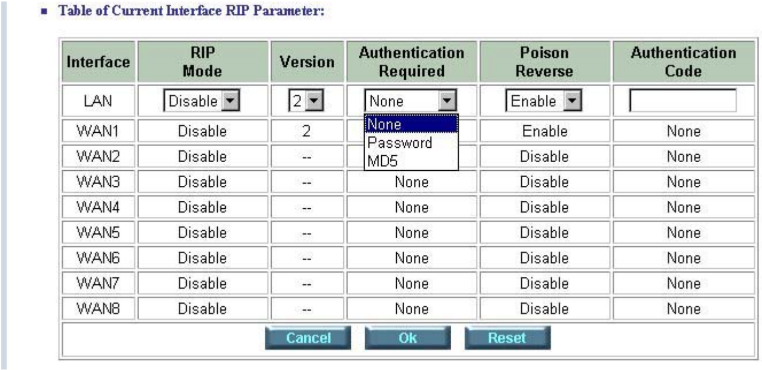
Interface	RIP Mode	Version	Authentication Required	Poison Reverse	Authentication Code
LAN	Disable	2	None	Enable	
WAN1	Disable		None	Enable	None
WAN2	Disable	--	None	Disable	None
WAN3	Disable	--	None	Disable	None
WAN4	Disable	--	None	Disable	None
WAN5	Disable	--	None	Disable	None
WAN6	Disable	--	None	Disable	None
WAN7	Disable	--	None	Disable	None
WAN8	Disable	--	None	Disable	None

Authentication required:

None: for RIP, there is no need of authentication code.

Password: the RIP is protected by password, authentication code.

MD5: The RIP will be decoded by MD5 than protected by password, authentication code.



▪ Table of Current Interface RIP Parameter:

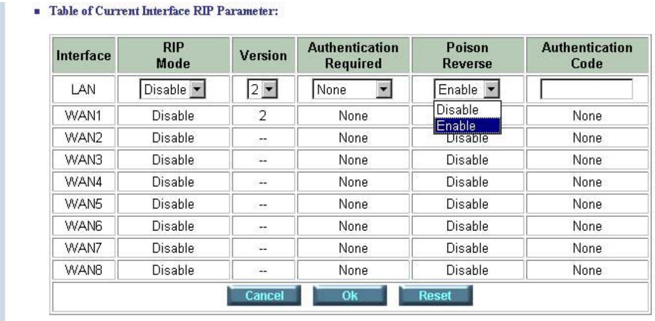
Interface	RIP Mode	Version	Authentication Required	Poison Reverse	Authentication Code
LAN	Disable	2	None	Enable	
WAN1	Disable	2		Enable	None
WAN2	Disable	--		Disable	None
WAN3	Disable	--	None	Disable	None
WAN4	Disable	--	None	Disable	None
WAN5	Disable	--	None	Disable	None
WAN6	Disable	--	None	Disable	None
WAN7	Disable	--	None	Disable	None
WAN8	Disable	--	None	Disable	None

Poison Reserve:

Poison Reserve is for the purpose of promptly broadcast or multicast the RIP while the route is changed. (ex shuting down one of the routers in routing table)

Enable: the gateway will actively broadcast or multicast the information.

Disable: the gateway will not broadcast or multicast the information.



▪ Table of Current Interface RIP Parameter:

Interface	RIP Mode	Version	Authentication Required	Poison Reverse	Authentication Code
LAN	Disable ▾	2 ▾	None ▾	Enable ▾ Disable Enable	
WAN1	Disable	2	None	[illegible]	None
WAN2	Disable	--	None	Disable	None
WAN3	Disable	--	None	Disable	None
WAN4	Disable	--	None	Disable	None
WAN5	Disable	--	None	Disable	None
WAN6	Disable	--	None	Disable	None
WAN7	Disable	--	None	Disable	None
WAN8	Disable	--	None	Disable	None

Authentication code:

You can set up a authentication code on here.

After modifying the RIP parameters, press finish.

The screen will prompt the modified parameter. Check the parameters and perss Restart to restart the router or press Continue to setup another parameters.

4.2.7 NAT/DMZ

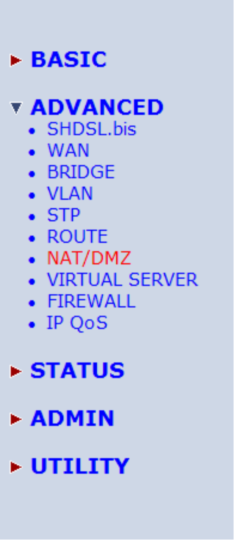
NAT *(Network Address Translation) is the translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network. One network is designated the inside network and the other is the outside. Typically, a company maps its local inside network addresses to one or more global outside IP addresses and reverse the global IP addresses of incoming packets back into local IP addresses. This ensure security since each outgoing or incoming request must go through a translation process, that also offers the opportunity to qualify or authenticate the request or match it to a previous request. NAT also conserves on the number of global IP addresses that a company needs and lets the company to use a single IP address of its communication in the Internet world.*

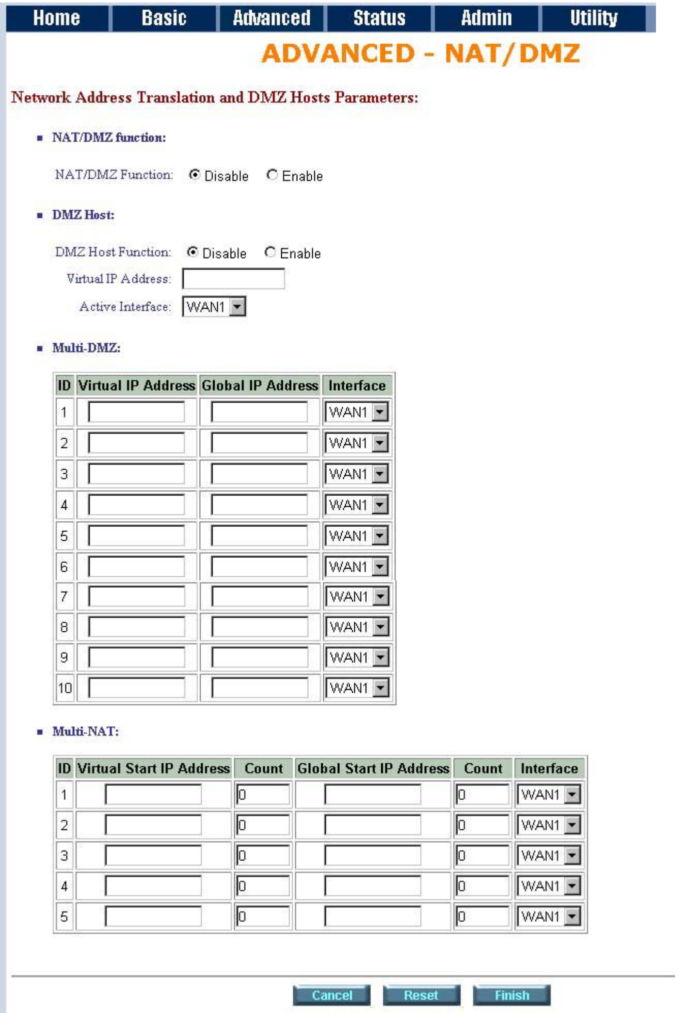
DMZ *(Demilitarized zone) is a computer host or small network inserted as a "neutral zone" between a company private network and the outside public network. It prevents outside users from getting direct access to a server that has company private data.*

In a typical DMZ configuration for an enterprise, a separate computer or host receives requests from users within the private network to access via Web sites or other companies accessible on the public network. The DMZ host then initiates sessions for these requests to the public network. However, the DMZ host is not able to initiate a session back into the private network. It can only forward packets that have already been requested.

Users of the public network outside the company can access only the DMZ host. The DMZ may typically also have the company's Web pages so these could serve the outside world. However, the DMZ provides access to no other company data. In the event that an outside user penetrated the DMZ host's security, the Web pages might be corrupted, but no other company information would be exposed.

Press NAT/DMZ to setup the parameters.





ADVANCED - NAT/DMZ

Network Address Translation and DMZ Hosts Parameters:

- NAT/DMZ function:

NAT/DMZ Function: ● Disable ○ Enable

- DMZ Host:

DMZ Host Function: ● Disable ○ Enable
Virtual IP Address:
Active Interface: WAN1

- Multi-DMZ:

ID	Virtual IP Address	Global IP Address	Interface
1			WAN1
2			WAN1
3			WAN1
4			WAN1
5			WAN1
6			WAN1
7			WAN1
8			WAN1
9			WAN1
10			WAN1

- Multi-NAT:

ID	Virtual Start IP Address	Count	Global Start IP Address	Count	Interface
1		0		0	WAN1
2		0		0	WAN1
3		0		0	WAN1
4		0		0	WAN1
5		0		0	WAN1

If you want to enable the NAT/DMZ functions, click Enable. Enable the DMZ host Function is used the IP address assigned to the WAN for enabling DMZ function for the virtual IP address.

4.2.7.1 Multi-DMZ

Some users who have two or more global IP addresses assigned by ISP can be used the multi DMZ. The table is for the mapping of global IP address and virtual IP address.

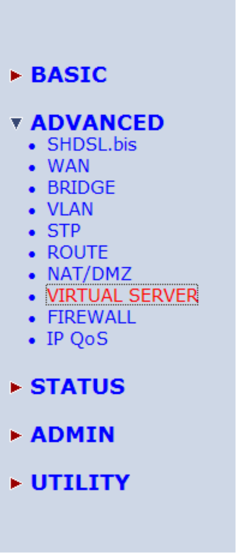
4.2.7.2 Mutli-NAT

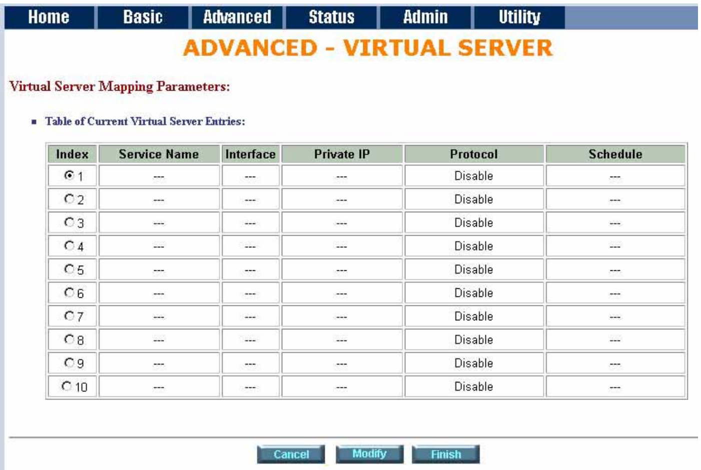
Some of the virtual IP addresses (eg: 192.168.0.10 ~ 192.168.0.50) collectively use two of the global IP addresses (eg: 69.210.1.9 and 69.210.1.10). The Multi-NAT table will be setup as;
Virtual Start IP Address: 192.168.0.10
Count: 40
Global Start IP Address: 69.210.1.9
Count: 2
Press Finish to continue to review.

The screen will prompt the parameters that will be written in NVRAM. Check the parameters before writing in NVRAM. Press Restart to restart the router working with new parameters or Continue to configure another parameter.

4.2.8 Virtual Server

Click Virtual Server to configure the parameters.





ADVANCED - VIRTUAL SERVER

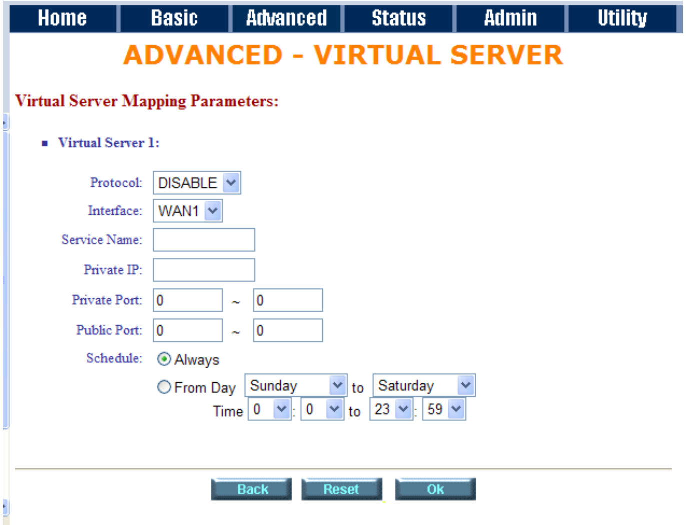
Virtual Server Mapping Parameters:

- Table of Current Virtual Server Entries:

Index	Service Name	Interface	Private IP	Protocol	Schedule
● 1	---	---	---	Disable	---
○ 2	---	---	---	Disable	---
○ 3	---	---	---	Disable	---
○ 4	---	---	---	Disable	---
○ 5	---	---	---	Disable	---
○ 6	---	---	---	Disable	---
○ 7	---	---	---	Disable	---
○ 8	---	---	---	Disable	---
○ 9	---	---	---	Disable	---
○ 10	---	---	---	Disable	---

There have ten virtual server index form 1 to 10 can been set up.

Press Modify for modify index 1.



ADVANCED - VIRTUAL SERVER

Virtual Server Mapping Parameters:

- Virtual Server 1:

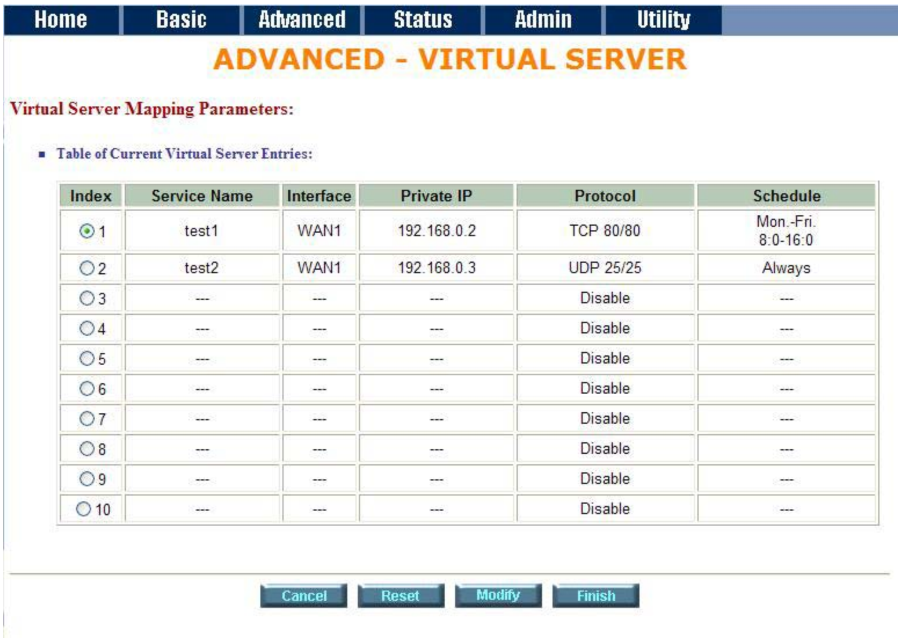
Protocol: DISABLE
Interface: WAN1
Service Name:
Private IP:
Private Port: 0 ~ 0
Public Port: 0 ~ 0
Schedule: ● Always
○ From Day Sunday to Saturday
Time 0 : 0 to 23 : 59

Type the necessary parameters and then click OK.

Press Restart to restart the router or press Continue to setup another function.

For example:

You can setup the router as Index 1, protocol TCP, interface WAN1, service name test1, private IP 192.168.0.2, private port 80, public port 80, schedule from Day Monday to Friday and time 8:0 to 16:0 and index 2, protocol UDP, interface WAN1, service name test2, private IP 192.168.0.3, private port 25, public port 25, schedule always.



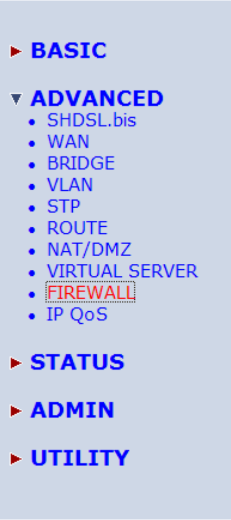
ADVANCED - VIRTUAL SERVER

Virtual Server Mapping Parameters:

- Table of Current Virtual Server Entries:

Index	Service Name	Interface	Private IP	Protocol	Schedule
● 1	test1	WAN1	192.168.0.2	TCP 80/80	Mon.-Fri. 8:0-16:0
○ 2	test2	WAN1	192.168.0.3	UDP 25/25	Always
○ 3	---	---	---	Disable	---
○ 4	---	---	---	Disable	---
○ 5	---	---	---	Disable	---
○ 6	---	---	---	Disable	---
○ 7	---	---	---	Disable	---
○ 8	---	---	---	Disable	---
○ 9	---	---	---	Disable	---
○ 10	---	---	---	Disable	---

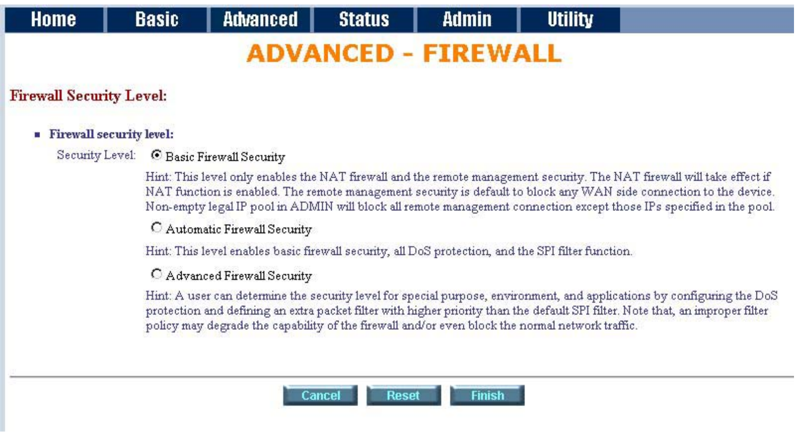
4.2.9 Firewall



A firewall is a set of related programs that protects the resources of a private network from other networks. It is helpful to users that allow preventing hackers to access its own private data resource accidentally.

There have three security levels for setting: **Basic firewall security**, **Automatic firewall security** and **advanced firewall security**.

4.2.9.1 Basic Firewall Security



ADVANCED - FIREWALL

Firewall Security Level:

- Firewall security level:

Security Level: ● Basic Firewall Security

Hint: This level only enables the NAT firewall and the remote management security. The NAT firewall will take effect if NAT function is enabled. The remote management security is default to block any WAN side connection to the device. Non-empty legal IP pool in ADMIN will block all remote management connection except those IPs specified in the pool.

○ Automatic Firewall Security

Hint: This level enables basic firewall security, all DoS protection, and the SPI filter function.

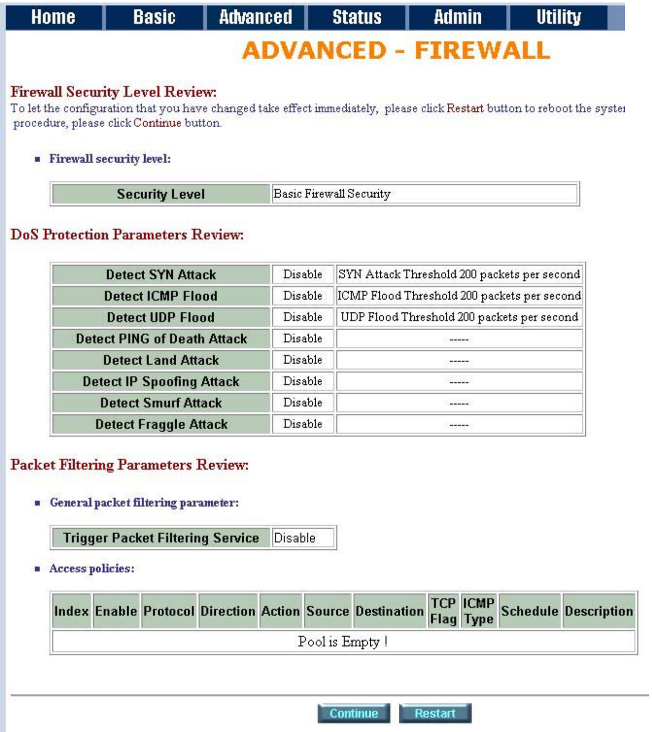
○ Advanced Firewall Security

Hint: A user can determine the security level for special purpose, environment, and applications by configuring the DoS protection and defining an extra packet filter with higher priority than the default SPI filter. Note that, an improper filter policy may degrade the capability of the firewall and/or even block the normal network traffic.

Click Basic Firewall Security.

This level only enables the NAT firewall and the remote management security. The NAT firewall will take effect if NAT function is enabled. The remote management security is default to block any WAN side connection to the device. Non-empty legal IP pool in ADMIN will block all remote management connection except those IPs specified in the pool.

Press Finish to finish setting of firewall and can review the parameters.



ADVANCED - FIREWALL

Firewall Security Level Review:

To let the configuration that you have changed take effect immediately, please click Restart button to reboot the syster
procedure, please click Continue button.

- Firewall security level:

Security Level	Basic Firewall Security

DoS Protection Parameters Review:

Detect SYN Attack	Disable	SYN Attack Threshold 200 packets per second
Detect ICMP Flood	Disable	ICMP Flood Threshold 200 packets per second
Detect UDP Flood	Disable	UDP Flood Threshold 200 packets per second
Detect PING of Death Attack	Disable	-----
Detect Land Attack	Disable	-----
Detect IP Spoofing Attack	Disable	-----
Detect Smurf Attack	Disable	-----
Detect Fraggle Attack	Disable	-----

Packet Filtering Parameters Review:

- General packet filtering parameter:

Trigger Packet Filtering Service	Disable

- Access policies:

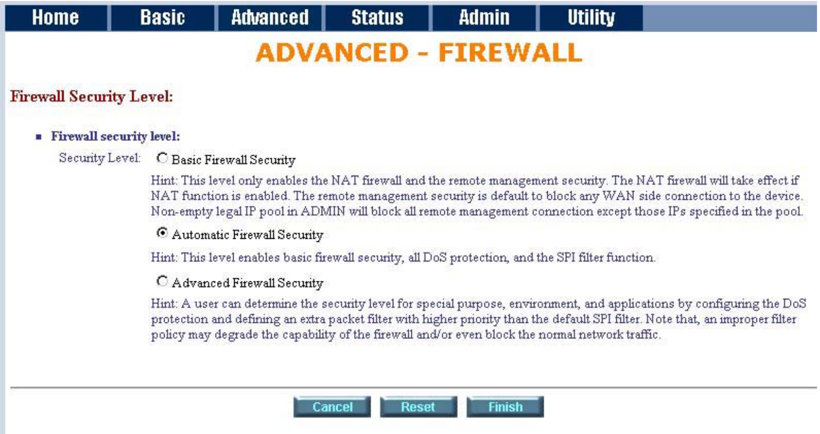
Index	Enable	Protocol	Direction	Action	Source	Destination	TCP Flag	ICMP Type	Schedule	Description
Pool is Empty !										

The screen will prompt the parameters, which router will record in NVRAM. Check the parameters.

Press Restart to restart the router or press Continue to setup another function.

4.2.9.2 Automatic Firewall Security

Click Automatic Firewall Security.



ADVANCED - FIREWALL

Firewall Security Level:

- Firewall security level:

Security Level: ○ Basic Firewall Security

Hint: This level only enables the NAT firewall and the remote management security. The NAT firewall will take effect if NAT function is enabled. The remote management security is default to block any WAN side connection to the device. Non-empty legal IP pool in ADMIN will block all remote management connection except those IPs specified in the pool.

● Automatic Firewall Security

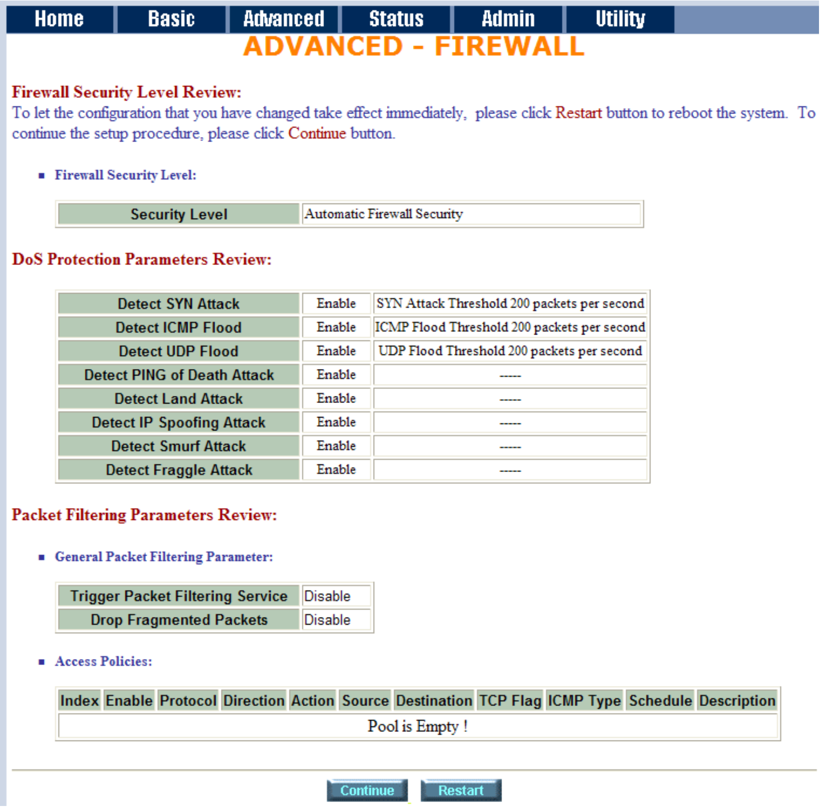
Hint: This level enables basic firewall security, all DoS protection, and the SPI filter function.

○ Advanced Firewall Security

Hint: A user can determine the security level for special purpose, environment, and applications by configuring the DoS protection and defining an extra packet filter with higher priority than the default SPI filter. Note that, an improper filter policy may degrade the capability of the firewall and/or even block the normal network traffic.

This level enables basic firewall security, all DoS protection, and the SPI filter function.

Press Finsih to finish setting firewall.



ADVANCED - FIREWALL

Firewall Security Level Review:

To let the configuration that you have changed take effect immediately, please click Restart button to reboot the system. To continue the setup procedure, please click Continue button.

- Firewall Security Level:

Security Level	Automatic Firewall Security

DoS Protection Parameters Review:

Detect SYN Attack	Enable	SYN Attack Threshold 200 packets per second
Detect ICMP Flood	Enable	ICMP Flood Threshold 200 packets per second
Detect UDP Flood	Enable	UDP Flood Threshold 200 packets per second
Detect PING of Death Attack	Enable	-----
Detect Land Attack	Enable	-----
Detect IP Spoofing Attack	Enable	-----
Detect Smurf Attack	Enable	-----
Detect Fraggle Attack	Enable	-----

Packet Filtering Parameters Review:

- General Packet Filtering Parameter:

Trigger Packet Filtering Service	Disable
Drop Fragmented Packets	Disable

- Access Policies:

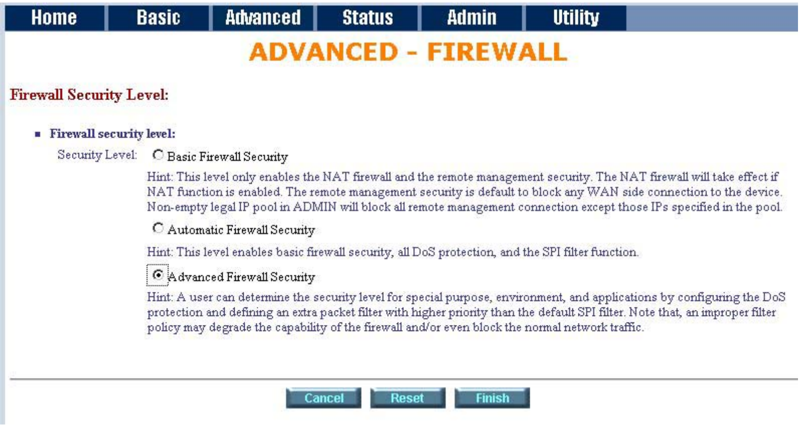
Index	Enable	Protocol	Direction	Action	Source	Destination	TCP Flag	ICMP Type	Schedule	Description
Pool is Empty !										

The screen will prompt the parameters, which will be written in NVRAM. Check the parameters. Press Restart to restart the router or press Continue to setup another function.

User can determine the security level for special purpose, environment, and applications by configuring the DoS protection and defining an extra packet filter. Note that, an improper filter policy may degrade the capability of the firewall and/or even block the normal network traffic.

4.2.9.3 Advanced Firewall Security

Click Advanced Firewall Security and then press Finish.



ADVANCED - FIREWALL

Firewall Security Level:

- Firewall security level:

Security Level: ○ Basic Firewall Security

Hint: This level only enables the NAT firewall and the remote management security. The NAT firewall will take effect if NAT function is enabled. The remote management security is default to block any WAN side connection to the device. Non-empty legal IP pool in ADMIN will block all remote management connection except those IPs specified in the pool.

○ Automatic Firewall Security

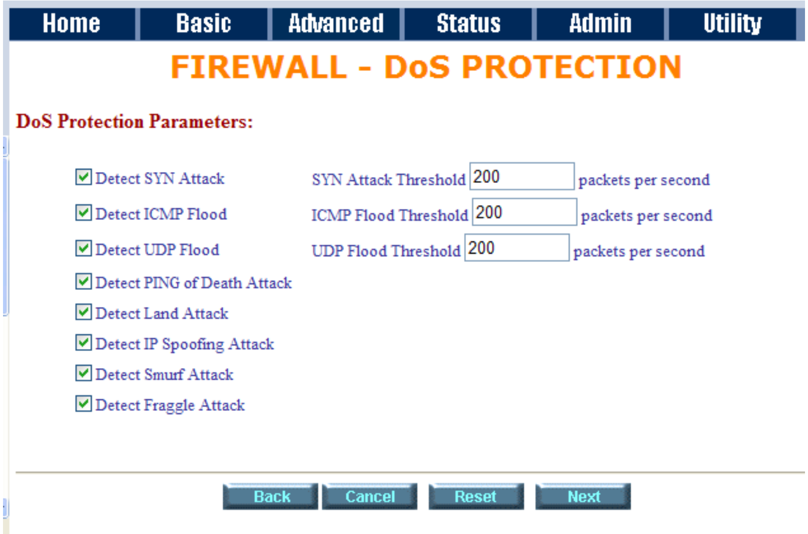
Hint: This level enables basic firewall security, all DoS protection, and the SPI filter function.

● Advanced Firewall Security

Hint: A user can determine the security level for special purpose, environment, and applications by configuring the DoS protection and defining an extra packet filter with higher priority than the default SPI filter. Note that, an improper filter policy may degrade the capability of the firewall and/or even block the normal network traffic.

A user can determine the security level for special purpose, environment and applications by configuring the DoS protection and defining an extra packet filter. Please notice that an improper filter policy may degrade the capability of the firewall and even block the normal network traffic.

It can set up the DoS protection parameters



FIREWALL - DoS PROTECTION

DoS Protection Parameters:

☑ Detect SYN Attack — SYN Attack Threshold 200 packets per second
☑ Detect ICMP Flood — ICMP Flood Threshold 200 packets per second
☑ Detect UDP Flood — UDP Flood Threshold 200 packets per second
☑ Detect PING of Death Attack
☑ Detect Land Attack
☑ Detect IP Spoofing Attack
☑ Detect Smurf Attack
☑ Detect Fraggle Attack

SYN flood: A SYN flood is a form of denial-of-service attack, attempts to slow your network by requesting new connections but not completing the process to open the connection. Once the buffer for these pending connections is full a server will not accept any more connections and will be unresponsive.

ICMP flood: A sender transmits a volume of ICMP request packets to cause all CPU resources to be consumed serving the phony requests.

UDP Flood: A UDP flood attack is a denial-of-service (DoS) attack using the User Datagram Protocol(UDP). A sender transmits a volume of requests for UDP diagnostic services which cause all CPU resources to be consumed serving the phony requests.

Ping of Death: A ping of death (abbreviated ”POD”) attack attempts to crash your system by sending a fragmented packet, when reconstructed is larger than the maximum allowable size.

Land attack: A land attack is an attempt to slow your network down by sending a packet with identical source and destination addresses originating from your network.

IP Spoofing: IP Spoofing is a method of masking the identity of an intrusion by making it appeared that the traffic came from a different computer. This is used by intruders to keep their anonymity and can be used in a Denial of Service attack.

Smurf attack: The Smurf attack is a way of generating a lot of computer network traffic to a victim host. That is a type of denial-of-service attack. A Smurf attack involves two systems. The attacker sends a packet containing a ICMP echo request (ping) to the network address of one system. This system is known as the amplifier. The return address of the ping has been faked (spoofed) to appear to come from a machine on another network (the victim). The victim is then flooded with responses to the ping. As many responses are generated for only one attack, the attacker is able use many amplifiers on the same victim.

Fraggle attack: A Fraggle attack is a type of denial-of-service attack where an attacker sends a large amount of UDP echo traffic to IP broadcast addresses, all of it having a fake source address. This is a simple rewrite of the smurf attack code.

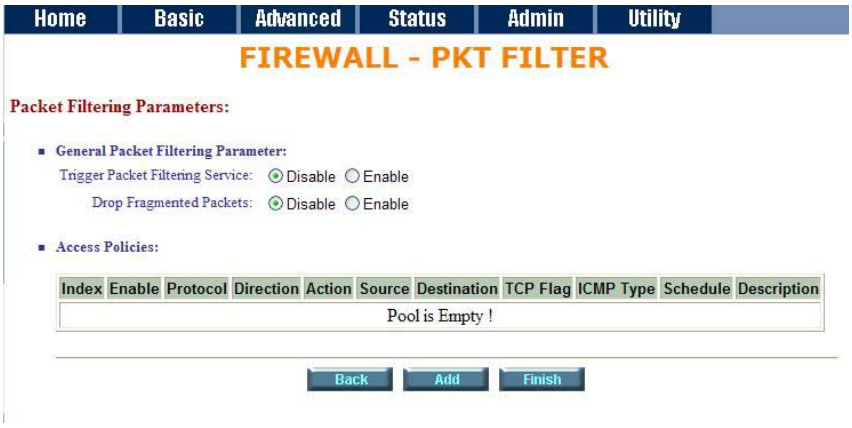
For SYN attack, ICMP flood and UDP flood, they can set up the threshold of packets number per second. The default values are 200 packets per second. If everything is working properly, you probably do not need to change the threshold setting as the default threshold values. Reduce the threshold values if your network is slower than average.

Traditional firewall is stateless meaning they have no memory of the connections of data or packets that pass through them. Such IP filtering firewalls simply examine header information in each packet and attempt to match it to a set of define rule. If the firewall finds a match, the prescribe action is taken. If no match is found, the packet is accepted into the network, or dropped, depending on the firewall configuration.

Packet filter

Click Next can set up the packet filtering parameters.

If you want to configure the Packet Filtering Parameters, choose **Enable** and press Add.



FIREWALL - PKT FILTER

Packet Filtering Parameters:

- General Packet Filtering Parameter:

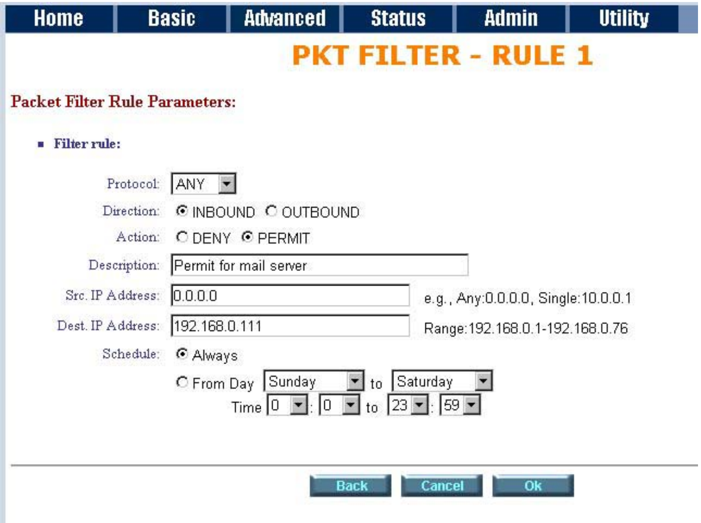
Trigger Packet Filtering Service: ● Disable ○ Enable

Drop Fragmented Packets: ● Disable ○ Enable

- Access Policies:

Index	Enable	Protocol	Direction	Action	Source	Destination	TCP Flag	ICMP Type	Schedule	Description
Pool is Empty !										

It can setup the packet filter rule parameters:



PKT FILTER - RULE 1

Packet Filter Rule Parameters:

- Filter rule:

Protocol: ANY

Direction: ● INBOUND ○ OUTBOUND

Action: ○ DENY ● PERMIT

Description: Permit for mail server

Src. IP Address: 0.0.0.0 e.g., Any:0.0.0.0, Single:10.0.0.1

Dest. IP Address: 192.168.0.111 Range:192.168.0.1-192.168.0.76

Schedule: ● Always

○ From Day Sunday to Saturday

Time 0 : 0 to 23 : 59

Select the Protocol and configure the parameter.

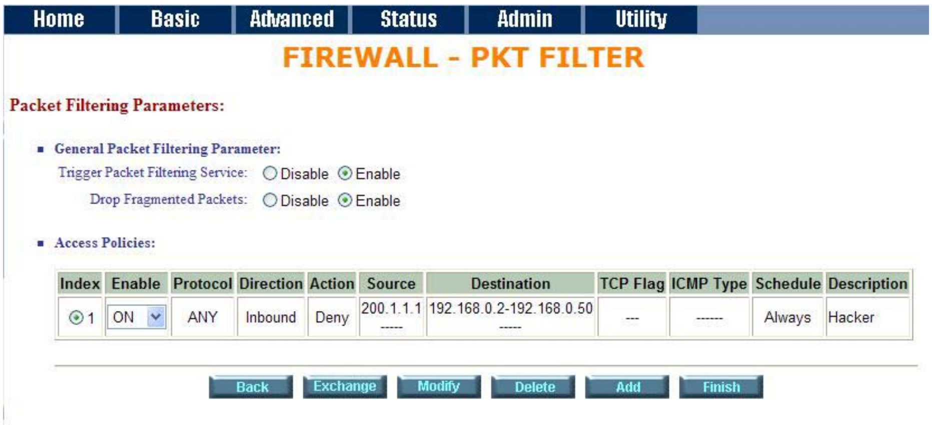
Protocol: ANY, TCP, UDP, ICMP, GRE, RSVP, ESP and AH.(ANY means all protocol)

TCP	Transmission Control Protocol
UDP	User Datagram Protocol
ICMP	Internet Control Message Protocol
GRE	Generic Routing Encapsulation
RSVP	Resource Reservation Protocol
ESP	Encapsulating Security Payload
AH	Authentication Header

Direction: INBOUND (from WAN to LAN) or OUTBOUND (from LAN to WAN)
Action: DENY(block) or PERMIT(allow)
Description: Type a description for your customized service..
Src. IP Address: The source addresses or ranges of addresses to which this packet filter rule applies. (Address 0.0.0.0 is equivalent Any)
Dest. IP Address: The destination addresses or ranges of addresses to which this packet filter rule applies. (Address 0.0.0.0 is equivalent Any)
Schedule: Select everyday (always) or the day(s) of the week to apply the rule. Enter the start and end times in the hour-minute format to apply the rule.

For example, If you want to ban all of the protocol from the IP (e.g.: 200.1.1.1) to access the all PCs (e.g.: 192.168.0.2 ~ 192.168.0.50) in the LAN, key in the parameter as:

Protocol: ANY
Direction: INBOUND (INBOUND is from WAN)
Action: DENY
Description: Hacker
Src. IP Address: 200.1.1.1
Dest. IP Address: 192.168.0.2-192.168.0.50
Schedule: You can set always or any time range which you want
Press OK to finish.



FIREWALL - PKT FILTER

Packet Filtering Parameters:

- General Packet Filtering Parameter:
  Trigger Packet Filtering Service: ○ Disable ● Enable
  Drop Fragmented Packets: ○ Disable ● Enable

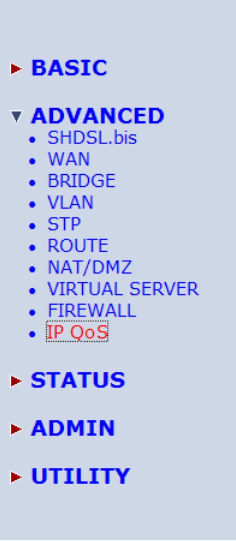
- Access Policies:

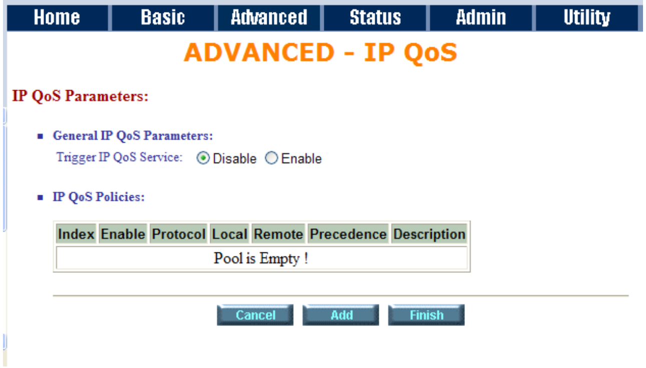
Index	Enable	Protocol	Direction	Action	Source	Destination	TCP Flag	ICMP Type	Schedule	Description
● 1	ON	ANY	Inbound	Deny	200.1.1.1 -----	192.168.0.2-192.168.0.50 -----	---	------	Always	Hacker

The screen will prompt the configured parameters.
Click Enable on Trigger Packet Filtering Service item, to active the packet filtering service.
Click Enable on Drop Fragmented Packets item, to active the drop fragmented packets operation.
You can modify or delete the access policies by click Modify or Delete command.

4.2.10 IP QoS

IP QoS is a function to decide the priorities of setting IPs to transfer packets under the situation of overloading bandwidth.





ADVANCED - IP QoS

IP QoS Parameters:

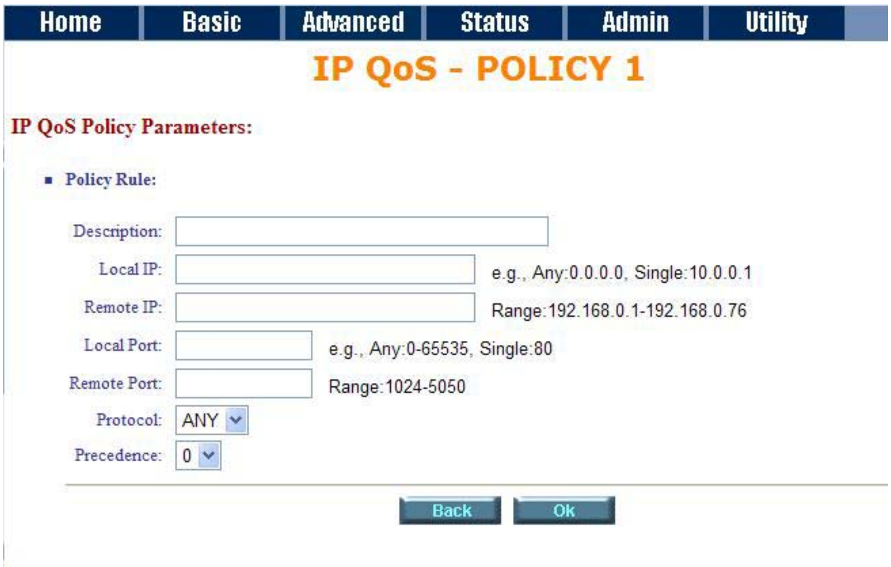
- General IP QoS Parameters:
  Trigger IP QoS Service: ● Disable ○ Enable

- IP QoS Policies:

Index	Enable	Protocol	Local	Remote	Precedence	Description
Pool is Empty !						

Click Enable at item Trigger IP QoS Service in General IP QoS Parameter, which will turn on this IP QoS function.

Click Add in the bottom of web page to begin a new entry in IP QoS Policy table.



IP QoS - POLICY 1

IP QoS Policy Parameters:

- Policy Rule:

Description:

Local IP: e.g., Any:0.0.0.0, Single:10.0.0.1

Remote IP: Range:192.168.0.1-192.168.0.76

Local Port: e.g., Any:0-65535, Single:80

Remote Port: Range:1024-5050

Protocol: ANY

Precedence: 0

Description: A brief statement describe this policy

Local IP: type IP address of local host in prioritized session.

Remote IP: type IP address of remote host in prioritized session.

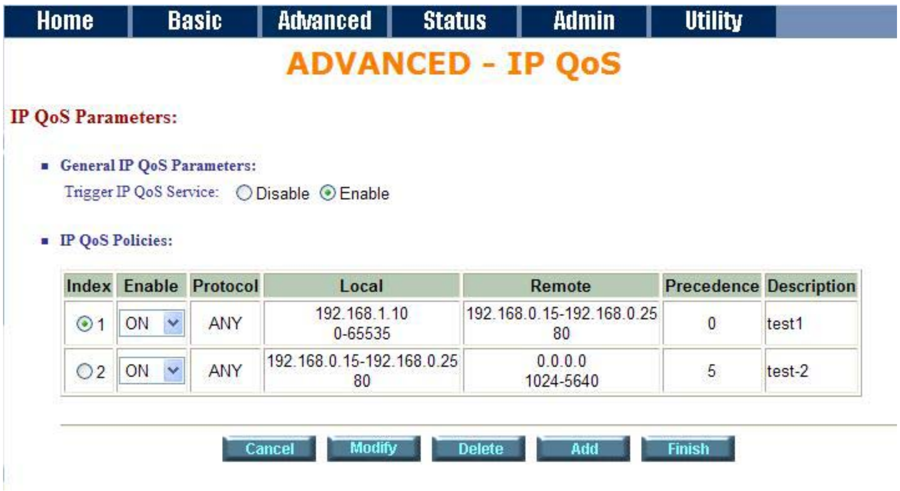
Local Port: type the service port number of local host in prioritized session.

Remote Port: type the service port number of remote host in prioritized session.

Protocol: identify the transportation layer protocol type you want to prioritize, ex: **TCP** or **UDP**. The default is **ANY**.

Precedence: type the session's prioritized level you classify, "**0**" is lowest priority, "**5**" is highest priority.

Click OK when all parameters are finish.



ADVANCED - IP QoS

IP QoS Parameters:

- General IP QoS Parameters:

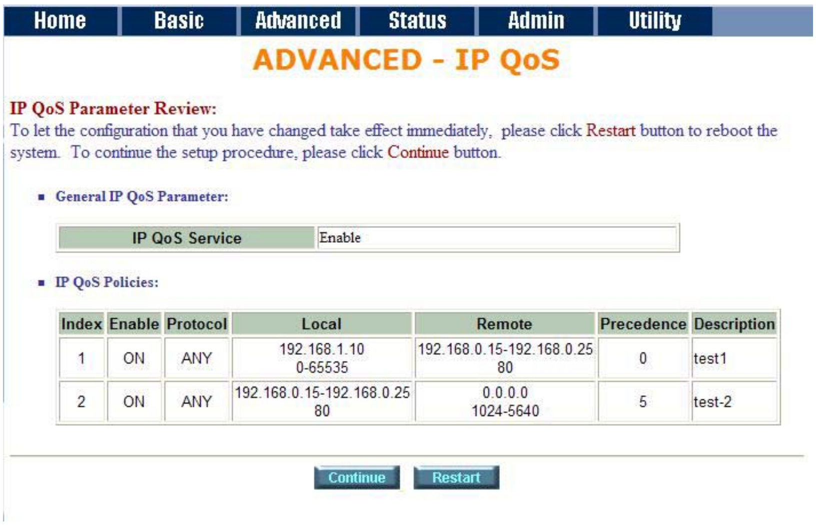
Trigger IP QoS Service: ○ Disable ● Enable

- IP QoS Policies:

Index	Enable	Protocol	Local	Remote	Precedence	Description
● 1	ON	ANY	192.168.1.10 0-65535	192.168.0.15-192.168.0.25 80	0	test1
○ 2	ON	ANY	192.168.0.15-192.168.0.25 80	0.0.0.0 1024-5640	5	test-2

You can modify or delete the policies by click Modify or Delete command

Click Finish can make a review for all IP QoS parameter



ADVANCED - IP QoS

IP QoS Parameter Review:
To let the configuration that you have changed take effect immediately, please click Restart button to reboot the system. To continue the setup procedure, please click Continue button.

- **General IP QoS Parameter:**

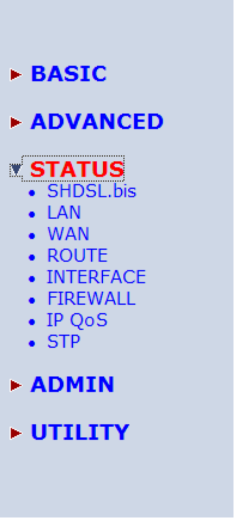
IP QoS Service	Enable

- **IP QoS Policies:**

Index	Enable	Protocol	Local	Remote	Precedence	Description
1	ON	ANY	192.168.1.10 0-65535	192.168.0.15-192.168.0.25 80	0	test1
2	ON	ANY	192.168.0.15-192.168.0.25 80	0.0.0.0 1024-5640	5	test-2

To let the IP QoS configuration you have changed and want those take effect immediately, please click Restart button to reboot the system. To continue the setup procedure, please click Continue button.

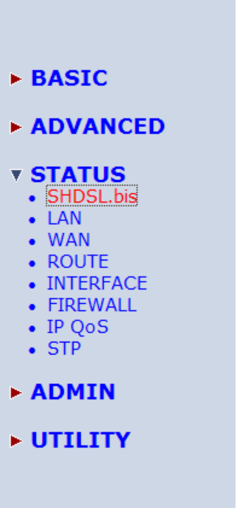
4.3 Status

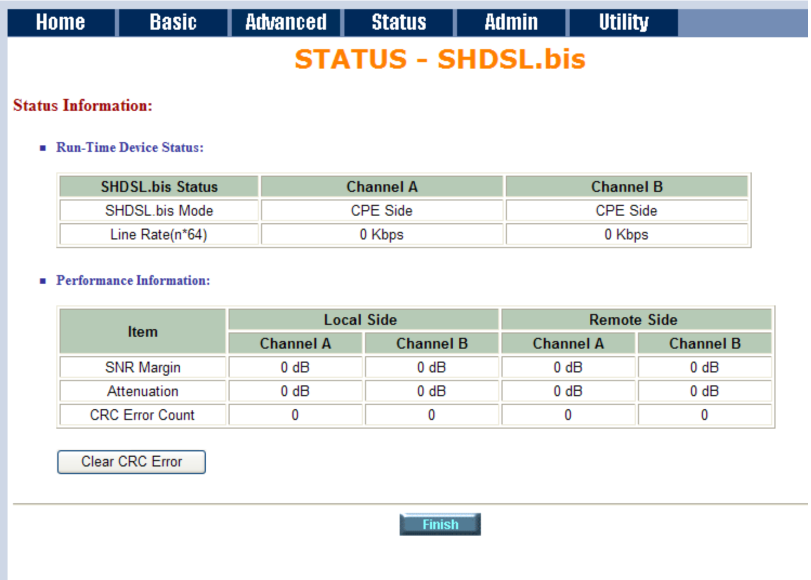


On STATUS item, you can monitor the following:

SHDSL.bis	Mode, Line rate and Performance information including SNR margin, atteunation and CRC error count.
LAN	IP type, MAC address, IP address, Subnet mask and DHCP client table: Type, IP address and MAC address.
WAN	WAN interface information. 8 WAN interface including IP address, Subnet Mask, VPI/VCI, Encapsulation, Protocol and Flag.
ROUTE	IP routing table including Flags, Destination IP/Netmask.Gateway, Interface and Portname.
INTERFACE	LAN and WAN statistics information.
FIREWALL	Current DoS protection status and dropped packets statistics.
IP QoS	Show IP QoS statistics on LAN interface
STP	STP information include Bridge parameter and Ports Parameter

4.3.1 SHDSL.bis





STATUS - SHDSL.bis

Status Information:

- Run-Time Device Status:

SHDSL.bis Status	Channel A	Channel B
SHDSL.bis Mode	CPE Side	CPE Side
Line Rate(n*64)	0 Kbps	0 Kbps

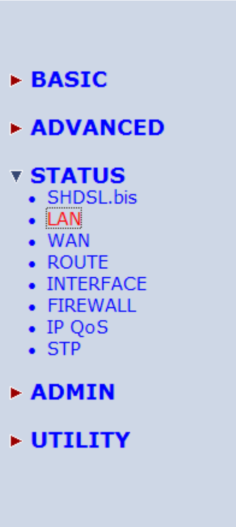
- Performance Information:

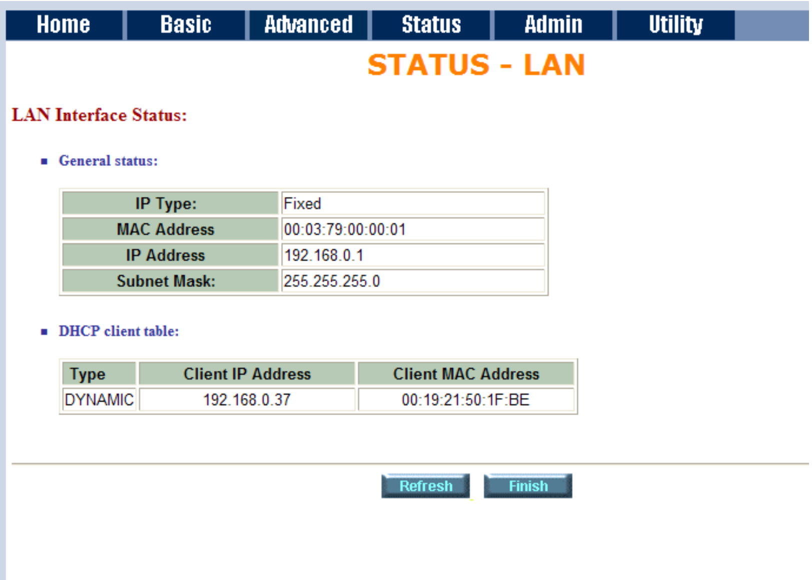
Item	Local Side		Remote Side	
	Channel A	Channel B	Channel A	Channel B
SNR Margin	0 dB	0 dB	0 dB	0 dB
Attenuation	0 dB	0 dB	0 dB	0 dB
CRC Error Count	0	0	0	0

The status information shows this is 4-wire model which have channel A and B. If the router have connected to remote side, it can also show the performance information of remote side.
It the router is 2-wire model, no any channel B information you can see.

Click Clear CRC Error can clear the CRC error count.

4.3.2 LAN





STATUS - LAN

LAN Interface Status:

- General status:

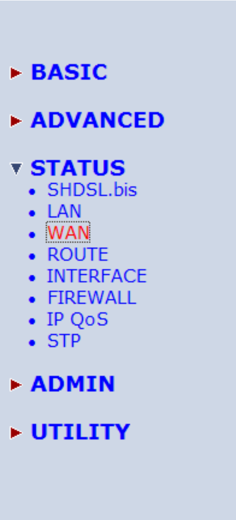
IP Type:	Fixed
MAC Address	00:03:79:00:00:01
IP Address	192.168.0.1
Subnet Mask:	255.255.255.0

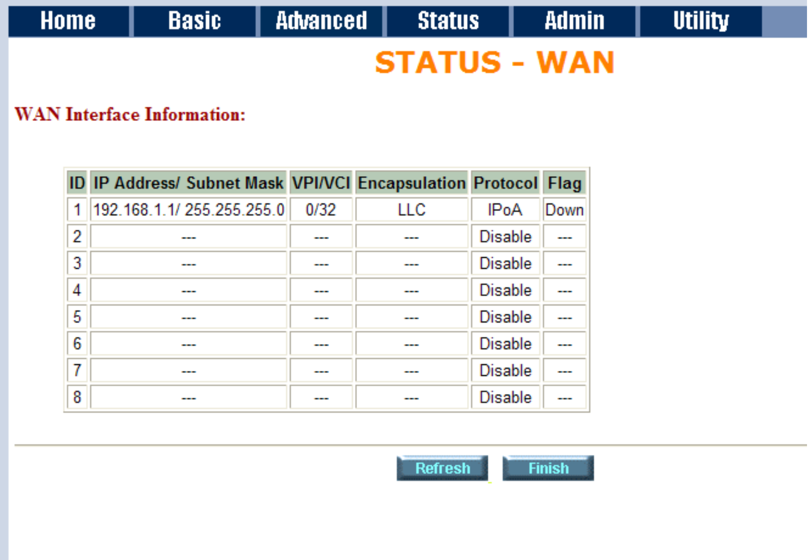
- DHCP client table:

Type	Client IP Address	Client MAC Address
DYNAMIC	192.168.0.37	00:19:21:50:1F:BE

This information shows the LAN interface status and DHCP client table.

4.3.3 WAN





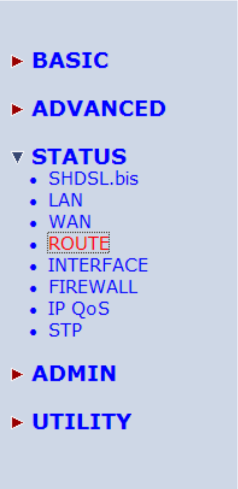
STATUS - WAN

WAN Interface Information:

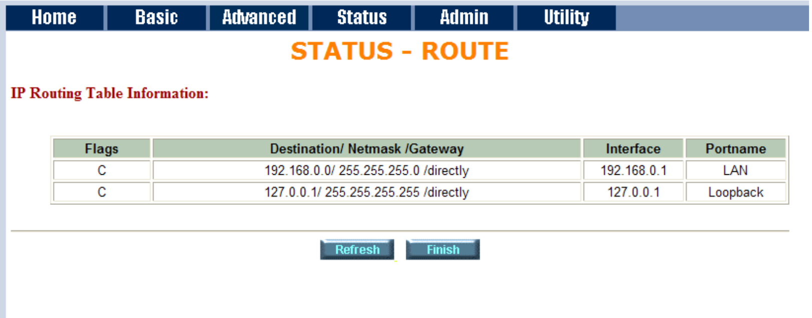
ID	IP Address/ Subnet Mask	VPI/VCI	Encapsulation	Protocol	Flag
1	192.168.1.1/ 255.255.255.0	0/32	LLC	IPoA	Down
2	---	---	---	Disable	---
3	---	---	---	Disable	---
4	---	---	---	Disable	---
5	---	---	---	Disable	---
6	---	---	---	Disable	---
7	---	---	---	Disable	---
8	---	---	---	Disable	---

This information shows all eight WAN interface.

4.3.4 ROUTE



Routing tables contain a list of IP address. Each IP address identifies a remote router (or other network gateway) that the local router is configured to recognize. For each IP address, the routing table additionally stores a network mask and other data that specifies the destination IP address ranges that remote device will accept.



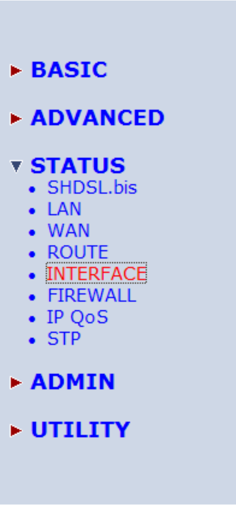
STATUS - ROUTE

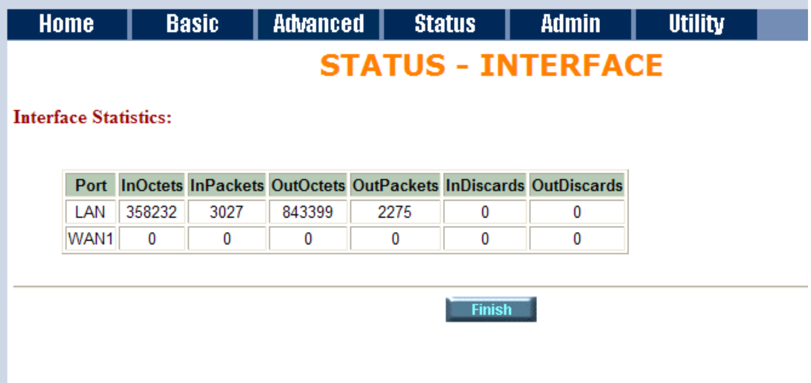
IP Routing Table Information:

Flags	Destination/ Netmask /Gateway	Interface	Portname
C	192.168.0.0/ 255.255.255.0 /directly	192.168.0.1	LAN
C	127.0.0.1/ 255.255.255.255 /directly	127.0.0.1	Loopback

This information shows the IP routing table.

4.3.5 INTERFACE





Interface Statistics:

Port	InOctets	InPackets	OutOctets	OutPackets	InDiscards	OutDiscards
LAN	358232	3027	843399	2275	0	0
WAN1	0	0	0	0	0	0

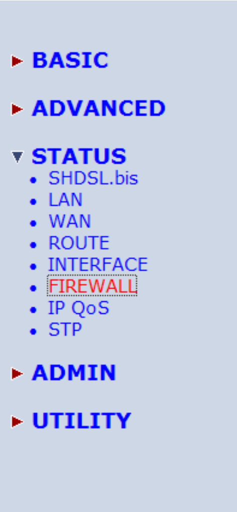
This table shows the interface statistics.

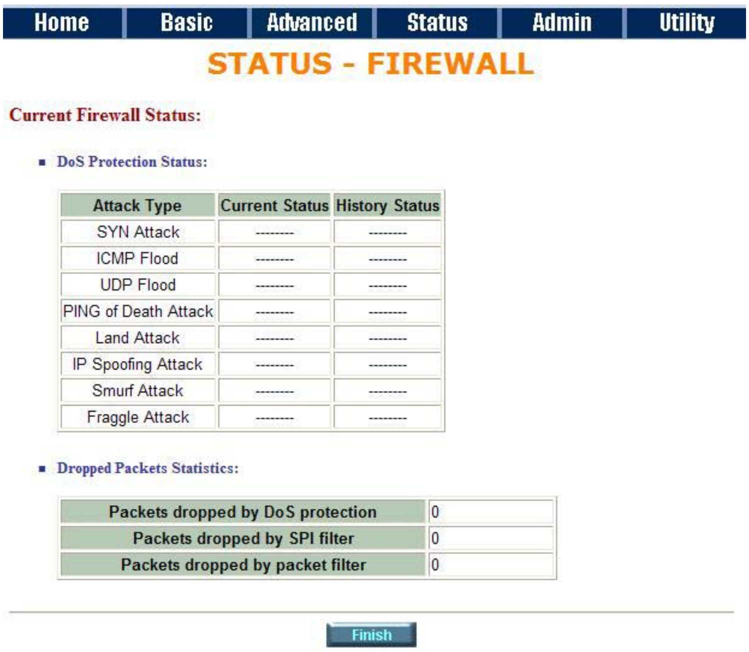
Octet is a group of 8 bits, often referred to as a byte.

Packet is a formatted block of data carried by a packet mode computer networks, often referred to the IP packet.

InOctets	The field shows the number of received bytes on this port
InPactets	The field shows the number of received packets on this port
OutOctets	The field shows the number of transmitted bytes on this port
OutPactets	The field shows the number of transmitted packets on this port
InDiscards	The field shows the discarded number of received packets on this port
OutDiscards	The field shows the discarded number of transmitted packets on this port

4.3.6 FIREWALL





STATUS - FIREWALL

Current Firewall Status:

- DoS Protection Status:

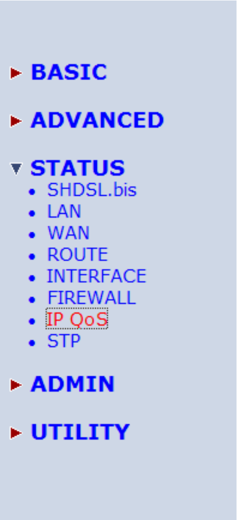
Attack Type	Current Status	History Status
SYN Attack	--------	--------
ICMP Flood	--------	--------
UDP Flood	--------	--------
PING of Death Attack	--------	--------
Land Attack	--------	--------
IP Spoofing Attack	--------	--------
Smurf Attack	--------	--------
Fraggle Attack	--------	--------

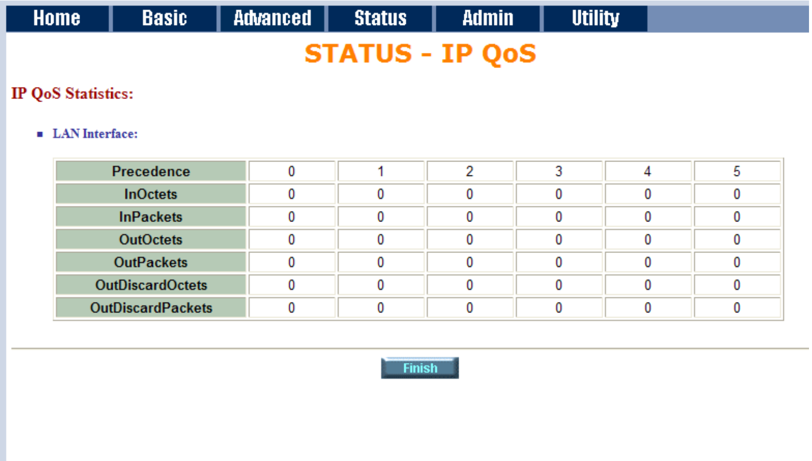
- Dropped Packets Statistics:

Packets dropped by DoS protection	0
Packets dropped by SPI filter	0
Packets dropped by packet filter	0

This information shows firewall status: DoS protection and dropped packets statistics.

4.3.7 IP QoS





STATUS - IP QoS

IP QoS Statistics:

- LAN Interface:

Precedence	0	1	2	3	4	5
InOctets	0	0	0	0	0	0
InPackets	0	0	0	0	0	0
OutOctets	0	0	0	0	0	0
OutPackets	0	0	0	0	0	0
OutDiscardOctets	0	0	0	0	0	0
OutDiscardPackets	0	0	0	0	0	0

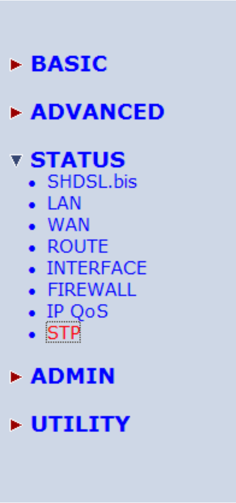
This information shows IP QoS statistics.

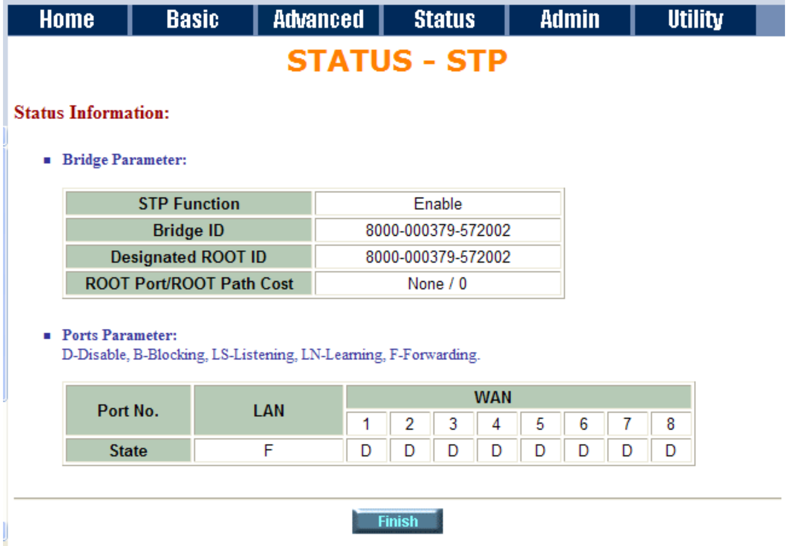
Octet is a group of 8 bits, often referred to as a byte.

Packet is a formatted block of data carried by a packet mode computer networks, often referred to the IP packet.

InOctets	The field shows the number of received bytes on this port
InPactets	The field shows the number of received packets on this port
OutOctets	The field shows the number of transmitted bytes on this port
OutPactets	The field shows the number of transmitted packets on this port
OutDiscardsOctets	The field shows the discarded number of transmitted bytes on this port
OutDiscardsPackets	The field shows the discarded number of transmitted packets on this port

4.3.8 STP





STATUS - STP

Status Information:

- Bridge Parameter:

STP Function	Enable
Bridge ID	8000-000379-572002
Designated ROOT ID	8000-000379-572002
ROOT Port/ROOT Path Cost	None / 0

- Ports Parameter:
  D-Disable, B-Blocking, LS-Listening, LN-Learning, F-Forwarding.

Port No.	LAN	WAN							
		1	2	3	4	5	6	7	8
State	F	D	D	D	D	D	D	D	D

This information shows the STP parameter:

The bridge parameters have:

Bridge ID: The bridge ID of a configuration message is an 8-byte field. The six low order bytes are the MAC address of the switch. The high order two-byte (unsigned 16-bit integer) field is the bridge priority number.

Designated Root ID: The unique Bridge Identifier of the Bridge assumed to be the Root, this parameter is used as the value of the Root Identifier parameter in all CBPDUs transmitted by the Bridge.

Root Port: Identifies the Port through which the path to the Root is established, and is not significant when the Bridge is the Root and is set to zero. It is the Port Identifier of the Port that offers the lowest Cost Path to the Root

Root Path Cost: The Cost of the Path to the Root from this Bridge, this is equal to the sum of the values of the Designated Cost and Path Cost parameters held for the Root Port. When the Bridge is the Root, this parameter is zero.

The ports parameters have:

Learning: This is when the modem creates a switching table that will map MAC addresses to port number.

Listening: This is when the modem processes BPDU’s that allow it to determine the network topology.

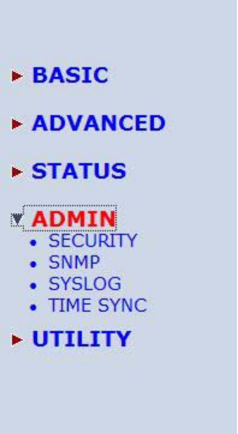
Forwarding: When a port receives or sends data. In other words, this is operating normally.

Disabled: This is when the network administrator has disabled the port.

Blocking: this means the port was blocked to stop a looping condition.

4.4 Administration

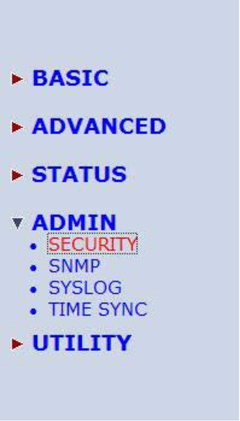
This session introduces security and simple network management protocol (SNMP) and time synchronous.



4.4.1 Security

For system secutiry, suggest to change the default user name and password in the first setup otherwise unauthorized persons can access the router and change the parameters.
There are three ways to configure the router: Web browser, telnet and serial console.

Press **Security** to setup the parameters.

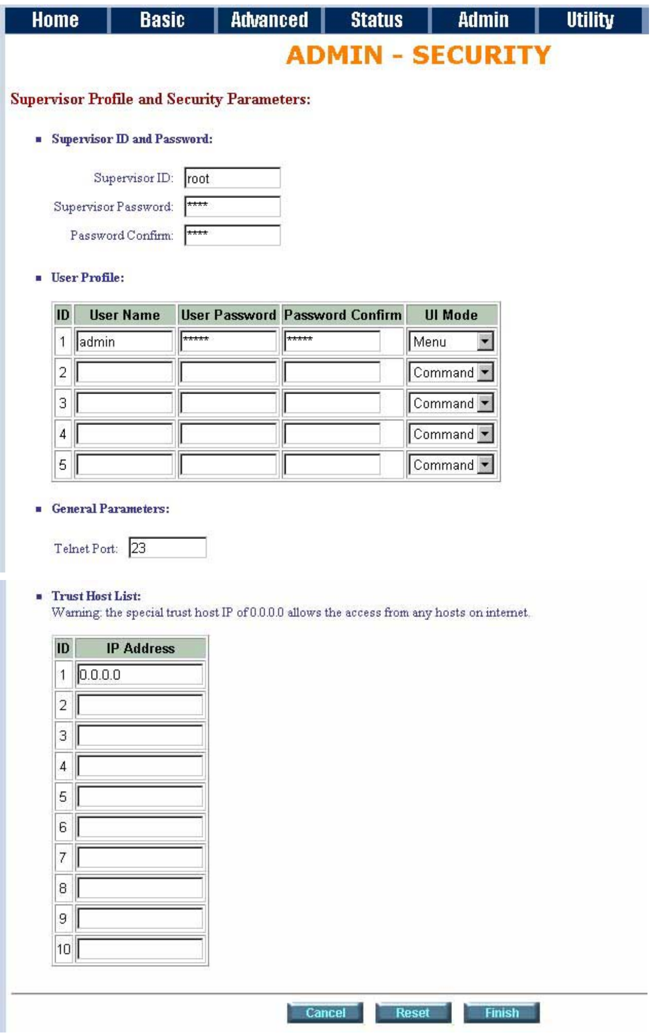


For greater security, change the Supervisor ID and password for the router. If you don't set them, all users on your network can be able to access the router using the default Supervisor IP and Supervisor Password is "***root***".

You can authorize five legal users to access the router via telnet or console only. There are two UI modes: **menu driven mode** and **line command mode** to configure the router. There are two UI modes, menu and command mode for telnet or console mode to setup the Router. The menu is meaning menu driven interface mode and Command is meaning line command mode. We will not discuss command mode in this manual.

The default user name on and Password are "***admin***".

Legal address pool will setup the legal IP addresses from which authorized person can configure the router. This is the more secure function for network administrator to setup the legal address of configuration.



ADMIN - SECURITY

Supervisor Profile and Security Parameters:

- Supervisor ID and Password:

Supervisor ID: root
Supervisor Password: ****
Password Confirm: ****

- User Profile:

ID	User Name	User Password	Password Confirm	UI Mode
1	admin	*****	*****	Menu
2				Command
3				Command
4				Command
5				Command

- General Parameters:

Telnet Port: 23

- Trust Host List:

Warning: the special trust host IP of 0.0.0.0 allows the access from any hosts on internet.

ID	IP Address
1	0.0.0.0
2	
3	
4	
5	
6	
7	
8	
9	
10	

This is the default supervisor ID and password is “***root***”. It is highly recommended that you change these for security purpose.

Supervisor ID: Type the new ID

Supervisor Password: Type the existing password (“***root***” is the default password when shipped)

Password Confirm: Retype your new password for confirmation.

Telnet Port: For Telnet, you may change the default service port by typing the new port number. If you change the default port number then you will have to let user who wish to use the service know the new port number. The default value is 23.

On trust host list, configured 0.0.0.0 will allow all hosts on Internet or LAN to access the router.

Leaving blank of trust host list will cause blocking all PC from WAN to access the router. On the other hand, only PC in LAN can access the router.

If you type the excact IP address in the filed, only the host on this listing can access to the router.

Click Finish to finish the setting.

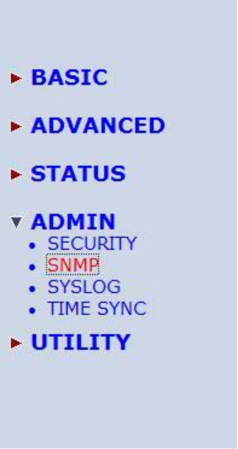
The browser will prompt the all configured parameters and check it before writing into NVRAM. Press Restart to restart the gateway working with the new parameters and press Continue to setup other parameters.

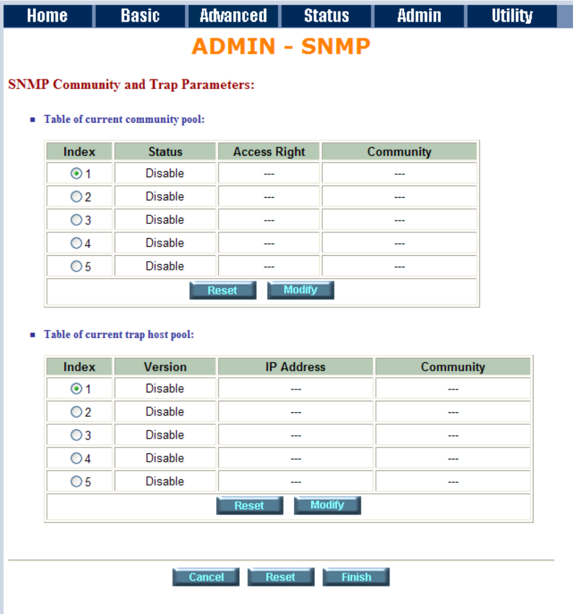
4.4.2 SNMP

Simple Network Management Protocol (SNMP) provides for the exchange of messages between a network management client and a network management agent for remote management of network nodes. These messages contain requests to get and set variables that exist in network nodes in order to obtain statistics, set configuration parameters, and monitor network events. SNMP communications can occur over the LAN or WAN connection.

The router can generate SNMP traps to indicate alarm conditions, and it relies on SNMP community strings to implement SNMP security.
This router support both MIB I and MIB II.

Click SNMP to configure the parameters.





ADMIN - SNMP

SNMP Community and Trap Parameters:

- Table of current community pool:

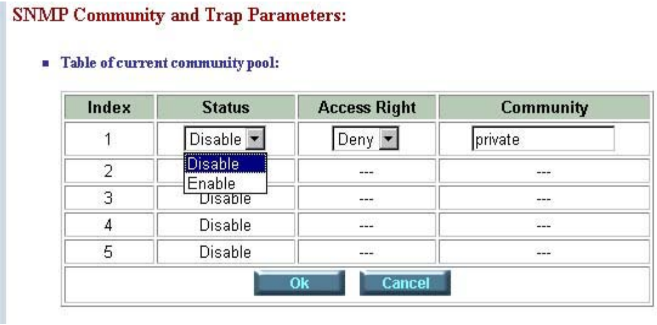
Index	Status	Access Right	Community
● 1	Disable	---	---
○ 2	Disable	---	---
○ 3	Disable	---	---
○ 4	Disable	---	---
○ 5	Disable	---	---

- Table of current trap host pool:

Index	Version	IP Address	Community
● 1	Disable	---	---
○ 2	Disable	---	---
○ 3	Disable	---	---
○ 4	Disable	---	---
○ 5	Disable	---	---

4.4.2.1 Community pool

Press Modify to modify the community pool. You can setup the access authority.

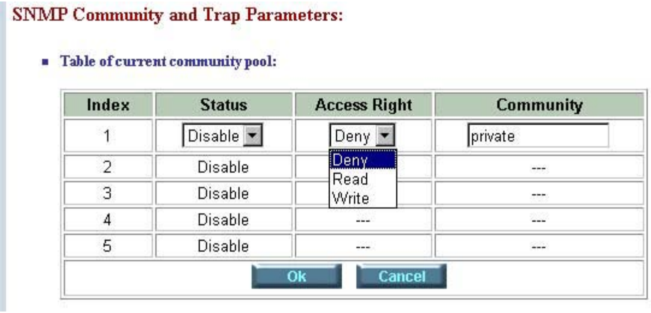


SNMP Community and Trap Parameters:

- Table of current community pool:

Index	Status	Access Right	Community
1	Disable	Deny	private
2		---	---
3	Disable	---	---
4	Disable	---	---
5	Disable	---	---

SNMP **Status**: Enable



SNMP Community and Trap Parameters:

- Table of current community pool:

Index	Status	Access Right	Community
1	Disable	Deny	private
2	Disable		---
3	Disable		---
4	Disable	---	---
5	Disable	---	---

Access Right: Deny for deny all access

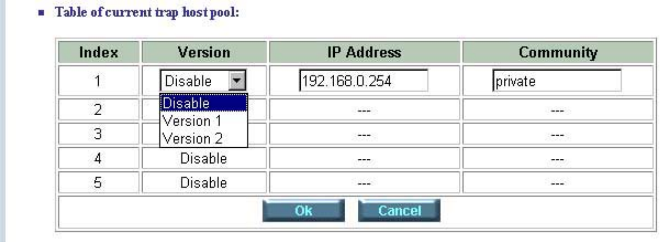
Read for access read only

Write for access read and write.

Community: it serves as password for access right.
After configuring the community pool, press OK.

4.4.2.2 Trap host pool

SNMP trap is an informational message sent from an SNMP agent to a manager. Click Modify to modify the trap host pool.



- Table of current trap host pool:

Index	Version	IP Address	Community
1	Disable	192.168.0.254	private
2		---	---
3		---	---
4	Disable	---	---
5	Disable	---	---

Version: select version for trap host. (Version 1 is for SNMPv1; Version 2 for SNMPv2).
IP Address: type the trap host IP address
Community: type the community password. The community is setup in community pool.

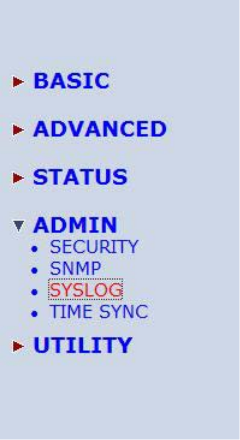
Press OK to finish the setup.

The browser will prompt the configured parameters and check it before writing into NVRAM.

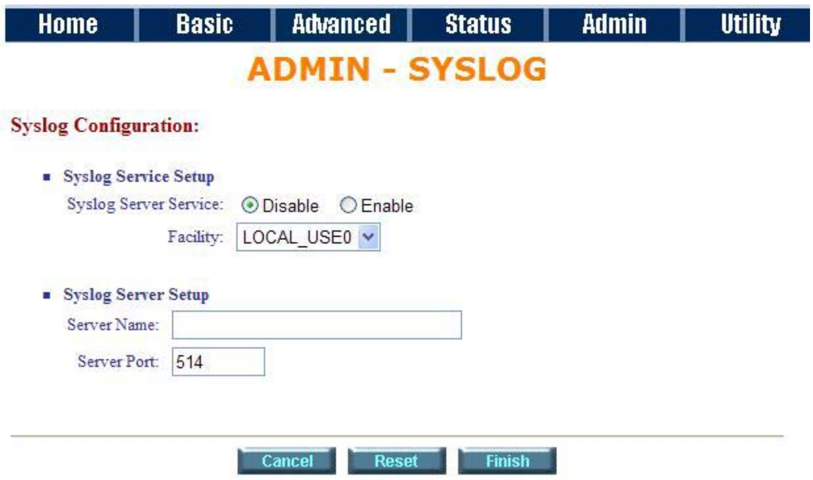
Press Restart to restart the gateway working with the new parameters and press Continue to setup other parameters.

4.4.3 SYSLOG

Syslog is a standard method of centralizing various logs. You can use a syslog server to store your servers logs in a remote location for later perusal or long-term storage.



Click SYSLOG to configure



ADMIN - SYSLOG

Syslog Configuration:

- Syslog Service Setup

Syslog Server Service: ● Disable ○ Enable

Facility: LOCAL_USE0

- Syslog Server Setup

Server Name:

Server Port: 514

To send logs to the LOG server, you must configure the other servers from your network to send logs to that server.

Syslog Service setup

1. Click the enable item of **Syslog Server Service** to turn on syslog service.

2. Select the syslog server facility. The log facility allows you to send logs to different files in the syslog server.

Syslog Server Setup

3. Specify an server name to which all syslog messages will be sent.

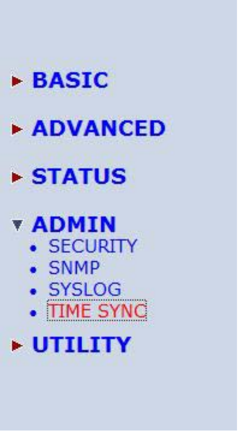
4. Specify a UDP port number to which the syslog server is listening. The default value is 514. Make sure this is not blocked from your firewall.

Press Finish to finish the setup. The browser will prompt the configured parameters and check it before writing into NVRAM.

4.4.4 Time Sync

Time synchronization is an essential element for any business, which relies on the IT system. The reason for this is that these systems all have clock that is the source of timer for their filing or operations. Without time synchronization, these system’s clocks vary and cause the failure of firewall packet filtering schedule processes, compromised security, or virtual server working in wrong schedule.

Click TIME SYNC.

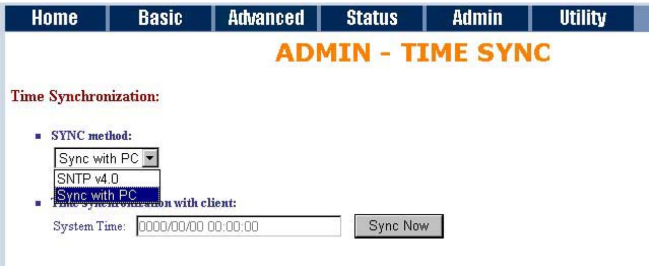


Time synchronization has two methods:

Sync with PC	Synchronization with PC
SNTP v4.0.	Simple Network Time Protocol with Version 4

4.4.4.1 Synchronization with PC

For synchronization with PC, select Sync with PC. The router will synchronize the time with the connecting PC. The function can supported on both bridge and router mode.



ADMIN - TIME SYNC

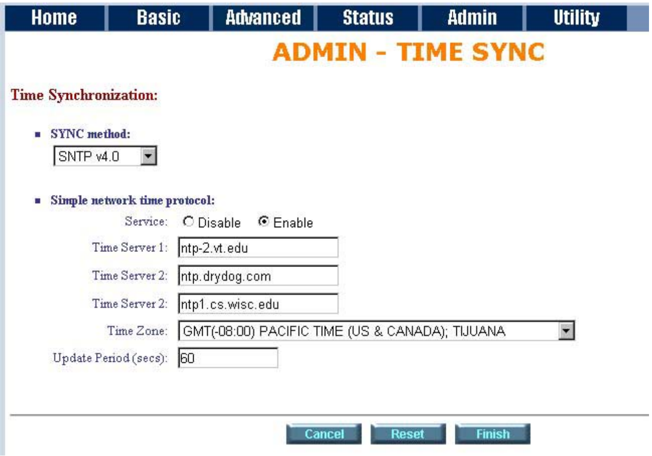
Time Synchronization:

- SYNC method: Sync with PC
- Time Synchronization with client:

System Time: 0000/00/00 00:00:00

4.4.4.2 SNTP v4.0

For using the SNTP, select SNTP v4.0.



ADMIN - TIME SYNC

Time Synchronization:

- SYNC method:
  SNTP v4.0
- Simple network time protocol:
  Service: ○ Disable ● Enable
  Time Server 1: ntp-2.vt.edu
  Time Server 2: ntp.drydog.com
  Time Server 2: ntp1.cs.wisc.edu
  Time Zone: GMT(-08:00) PACIFIC TIME (US & CANADA); TIJUANA
  Update Period (secs): 60

SNTP is the acronym for Simple Network Time Protocol, which is an adaptation of the Network Time Protocol (NTP) used to synchronize computer clocks in the Internet. SNTP can be used when the ultimate performance of the full NTP implementation. The function only supported on router mode.

Service: Enable

Time Server 1, Time Server 2 and Time Server 3: All of the time server around the world can be used but suggest using the time server nearby to your country. You can set up maximum three time server on here.

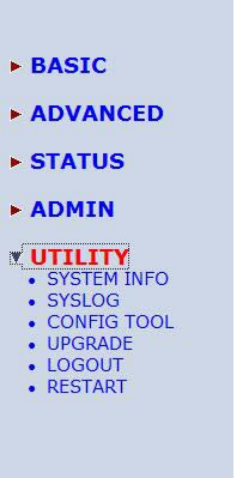
Time Zone: Select the time difference between UTC(Universal Time Coordinated, formerly known as GMT, Greenwich Mean Time) and your time zone from the drop-down list box.

Update Period: How many times the router can resynchronize to time server. The unit is second.

Press Finish to finish the setup. The browser will prompt the configured parameters and check it before writing into NVRAM.

.

4.5 Utility

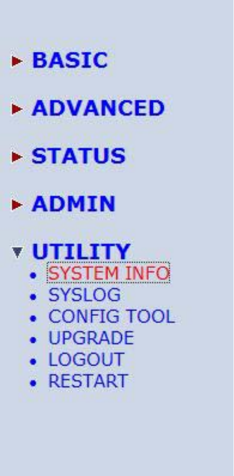


This section will describe the utility of the product including:

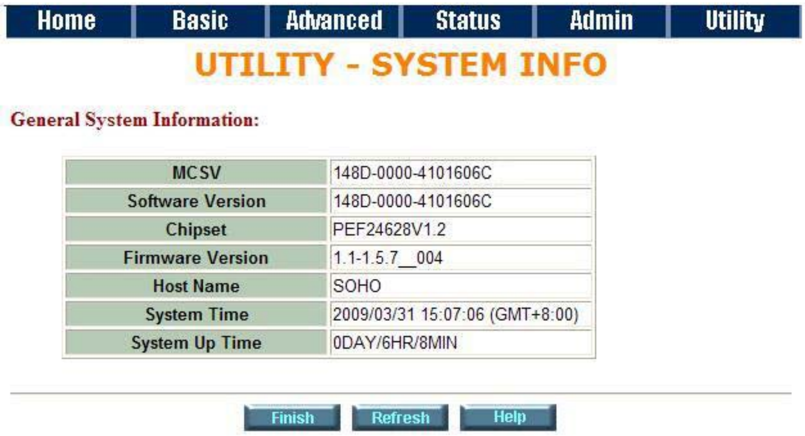
SYSTEM INFO	Show the system information
SYSLOG	Capturing log information
CONFIG TOOL	Load the factory default configuration, restore configuration and backup configuration
UPGRADE	Upgrade the firmware
LOGOUT	Logout the system
RESTART	Restart the router.

4.5.1 System Info

Click System Info for review the information.



The browser will prompt the system information.



UTILITY - SYSTEM INFO

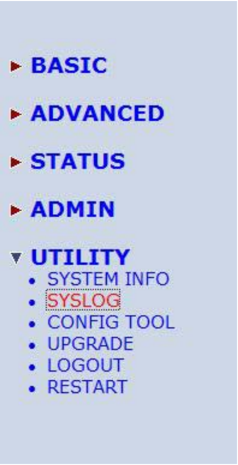
General System Information:

MCSV	148D-0000-4101606C
Software Version	148D-0000-4101606C
Chipset	PEF24628V1.2
Firmware Version	1.1-1.5.7__004
Host Name	SOHO
System Time	2009/03/31 15:07:06 (GMT+8:00)
System Up Time	0DAY/6HR/8MIN

There will display general system information including: MCSV, software version, chipset, firmware version, Host Name, System Time and System Up Time.

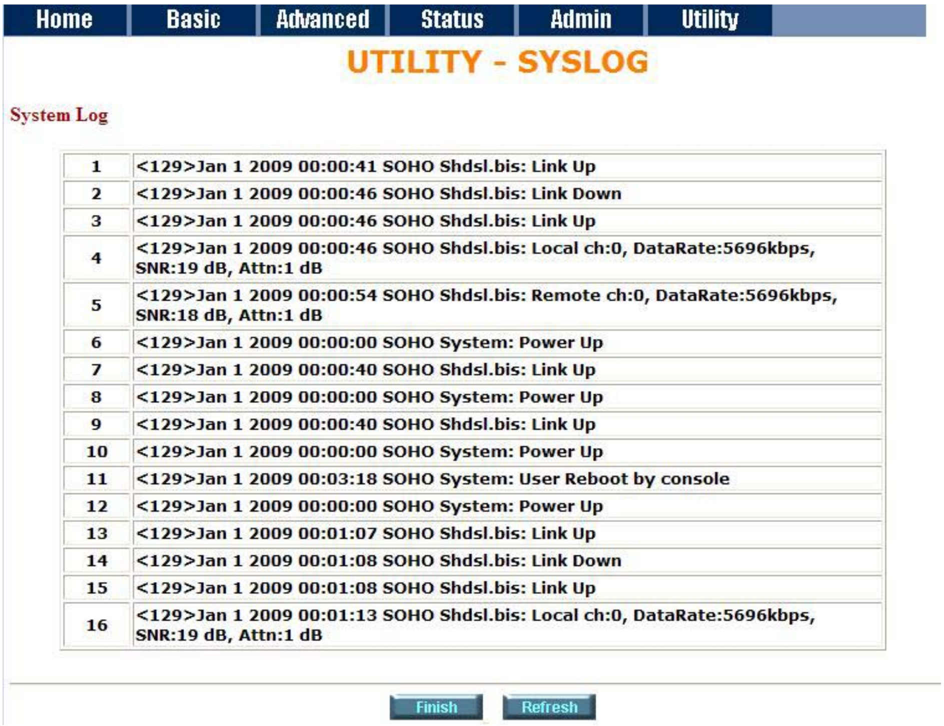
MCSV: For internal identification purposes.
Software Version: This is the modem's firmware version. This is sometimes needed by technicians to help troubleshoot problems.
Chipset: This is the SHDSL.bis chipset model name.
Firmware Version: This is the chipset's firmware version.
Host Name: This is the system name you enter in BASIC Setup. It is for identification purposes.
System Time: This field display your modem's present date and time.
System Up Time: This is the total time on the modem has been on.

4.5.2 SYSLOG



SHDSL.bis routers support detailed logging via Syslog function. The syslog protocol allows devices to send event notification messages across an IP network to syslog servers that collect the event message. The router can generate a syslog message and send it to a syslog server.

Press SYSLOG, it send the syslog messages shown as follows:

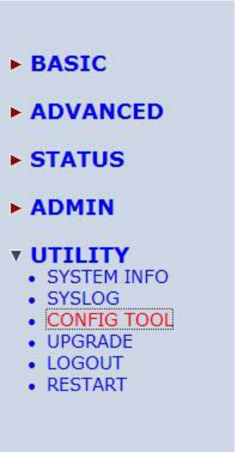


UTILITY - SYSLOG

System Log

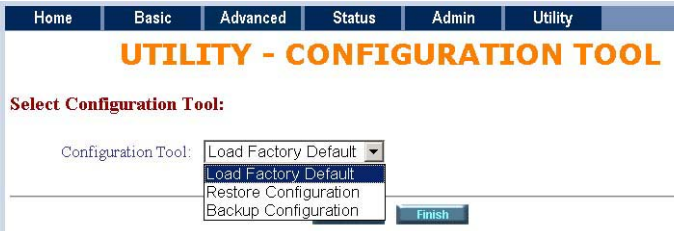
```
1   <129>Jan 1 2009 00:00:41 SOHO Shdsl.bis: Link Up
2   <129>Jan 1 2009 00:00:46 SOHO Shdsl.bis: Link Down
3   <129>Jan 1 2009 00:00:46 SOHO Shdsl.bis: Link Up
4   <129>Jan 1 2009 00:00:46 SOHO Shdsl.bis: Local ch:0, DataRate:5696kbps,
    SNR:19 dB, Attn:1 dB
5   <129>Jan 1 2009 00:00:54 SOHO Shdsl.bis: Remote ch:0, DataRate:5696kbps,
    SNR:18 dB, Attn:1 dB
6   <129>Jan 1 2009 00:00:00 SOHO System: Power Up
7   <129>Jan 1 2009 00:00:40 SOHO Shdsl.bis: Link Up
8   <129>Jan 1 2009 00:00:00 SOHO System: Power Up
9   <129>Jan 1 2009 00:00:40 SOHO Shdsl.bis: Link Up
10  <129>Jan 1 2009 00:00:00 SOHO System: Power Up
11  <129>Jan 1 2009 00:03:18 SOHO System: User Reboot by console
12  <129>Jan 1 2009 00:00:00 SOHO System: Power Up
13  <129>Jan 1 2009 00:01:07 SOHO Shdsl.bis: Link Up
14  <129>Jan 1 2009 00:01:08 SOHO Shdsl.bis: Link Down
15  <129>Jan 1 2009 00:01:08 SOHO Shdsl.bis: Link Up
16  <129>Jan 1 2009 00:01:13 SOHO Shdsl.bis: Local ch:0, DataRate:5696kbps,
    SNR:19 dB, Attn:1 dB
```

4.5.3 Config Tool



This configuration tool has three functions: load Factory Default, Restore Configuration, and Backup Configuration.

Press CONFIG TOOL.



UTILITY - CONFIGURATION TOOL

Select Configuration Tool:

Configuration Tool: Load Factory Default

Choose the function and then press Finish

4.5.3.1 Load Factory Default

Load Factory Default: It will load the factory default parameters to the router.

Note: This action will change all of the settings to factory default value. On the other hand, you will lose all the existing configured parameters.

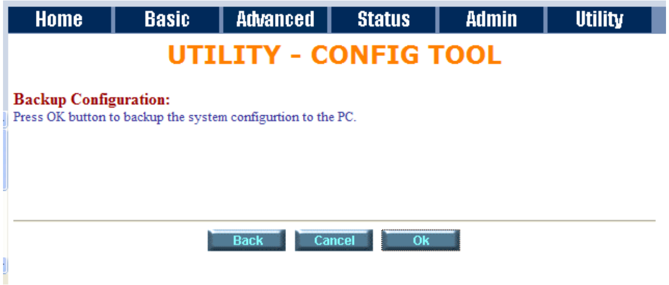
4.5.3.2 Restore Configuration

Sometime the configuration crushed occasionally. It will help you to recover the backup configuration easily.

Click Finish after selecting Restore Configuration.
Browse the route of backup file then press Finish. Brower the place of restore file name or put the name. Then press OK. The router will automatically restore the saved configuration.

4.5.3.3 Backup Configuration

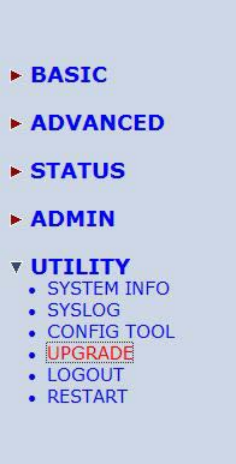
After configuration, suggest using the function to backup your router parameters in the PC. Select the Backup Configuration and then press Finish. Browse the place of backup file name or put the name. Then press OK. The router will automatically backup the configuration. If you don't put the file name, the system will use the default: *config1.log*

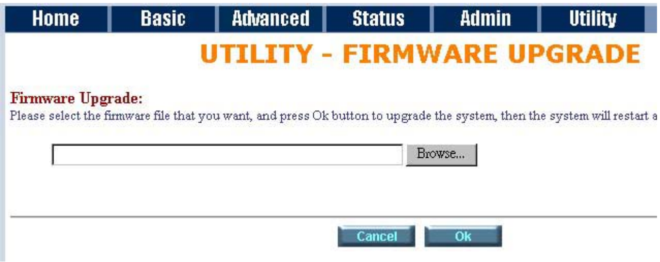


Backup Configuration:
Press OK button to backup the system configurtion to the PC.

4.5.4 Upgrade

You can upgrade the gateway using the upgrade function.
Press Upgrade in UTILITY.





UTILITY - FIRMWARE UPGRADE

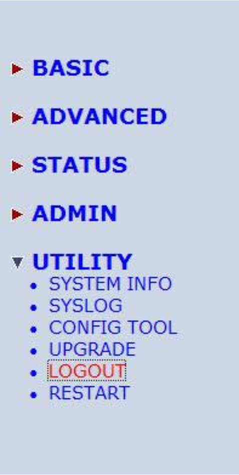
Firmware Upgrade:

Please select the firmware file that you want, and press Ok button to upgrade the system, then the system will restart a

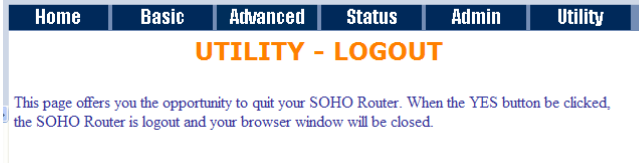
Select the firmware file name by click Browse on your PC or NB and press OK button to upgrade. The system will reboot automatically after finish the firmware upgrade operation.

4.5.5 Logout

To logout the router, press LOGOUT in UTILITY.



For logout system and close window, click the LOGOUT in UTILITY



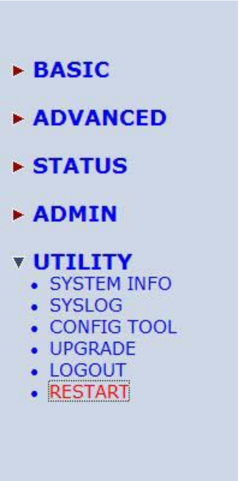
UTILITY - LOGOUT

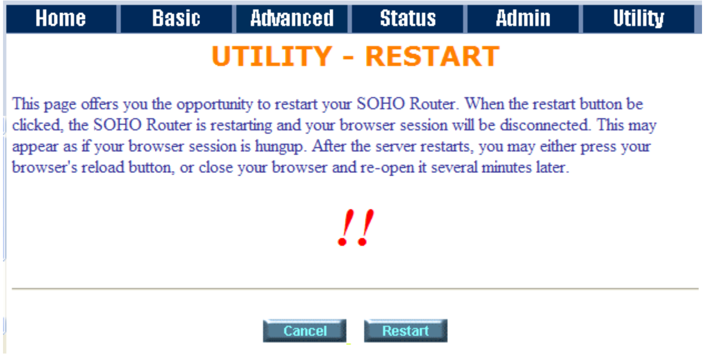
This page offers you the opportunity to quit your SOHO Router. When the YES button be clicked, the SOHO Router is logout and your browser window will be closed.

When click the Yes button, the Router will logout and browser window will be closed.

4.5.6 Restart

For restarting the router, click the RESTART in UTILITY.





UTILITY - RESTART

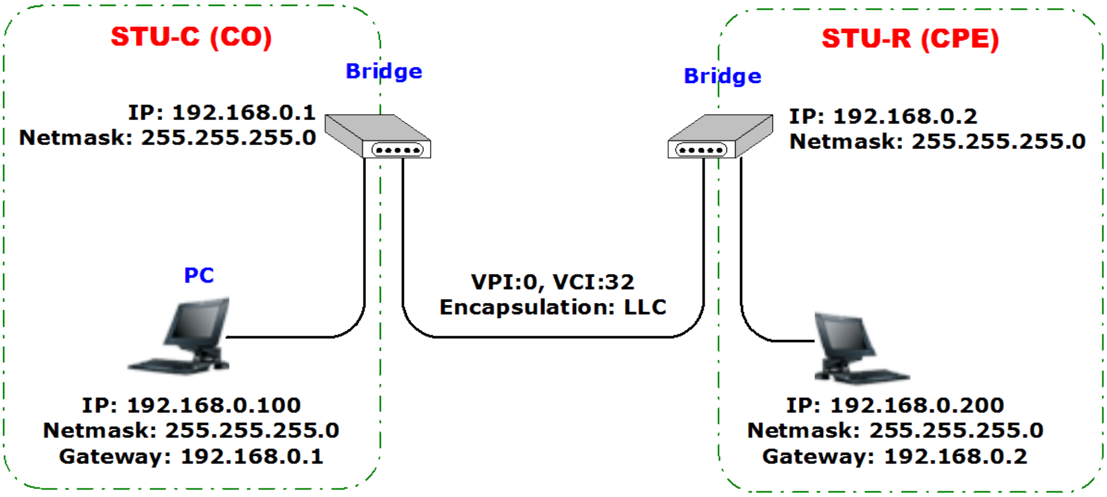
This page offers you the opportunity to restart your SOHO Router. When the restart button be clicked, the SOHO Router is restarting and your browser session will be disconnected. This may appear as if your browser session is hungup. After the server restarts, you may either press your browser's reload button, or close your browser and re-open it several minutes later.

Press Restart to reboot the router.

When the restart button been clicked, the router will restarting and the browser session will be disconnected. This may appear as if your browser session is hung up. After the router restarts, you may either click the browser’s reload button or close the browser and re-open it later.

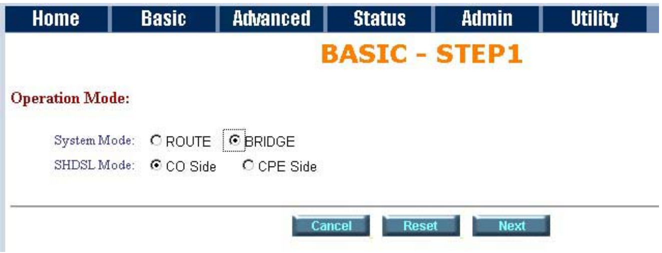
4.6 Example

4.6.1 LAN-to-LAN connection with bridge Mode



4.6.1.1 *CO side*

Click Bridge and CO Side to setup Bridging mode of the Router and then click Next.

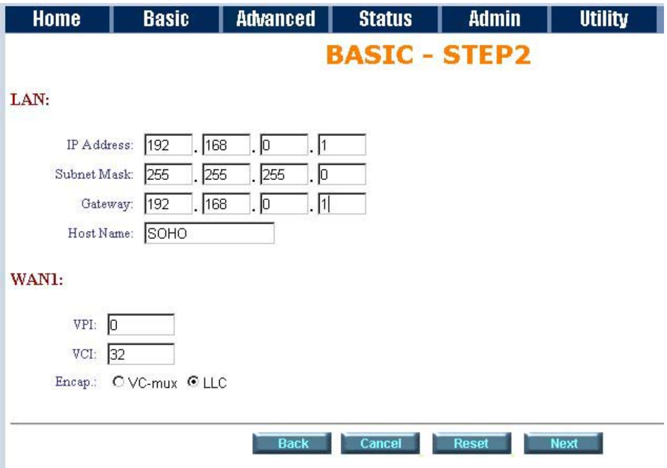


BASIC - STEP1

Operation Mode:

System Mode: ○ ROUTE ● BRIDGE

SHDSL Mode: ● CO Side ○ CPE Side



BASIC - STEP2

LAN:

IP Address: 192 . 168 . 0 . 1

Subnet Mask: 255 . 255 . 255 . 0

Gateway: 192 . 168 . 0 . 1

Host Name: SOHO

WAN1:

VPI: 0

VCI: 32

Encap.: ○ VC-mux ● LLC

Enter **LAN** Parameters

IP: 192.168.0.1

Subnet Mask: 255.255.255.0

Gateway: 192.168.0.1

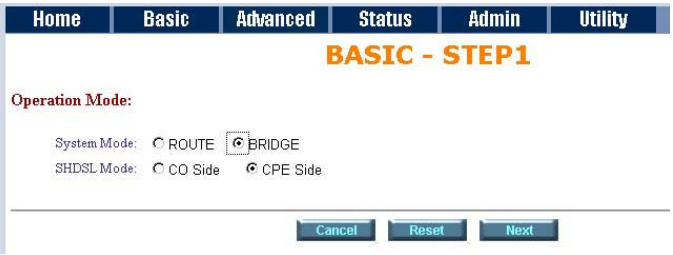
Host Name: SOHO

Enter **WAN1** Parameters
VPI: 0
VCI: 32
Click LLC
Click Next

The screen will prompt the new configured parameters. Check the parameters and Click Restart The router will reboot with the new setting.

4.6.1.2 CPE Side

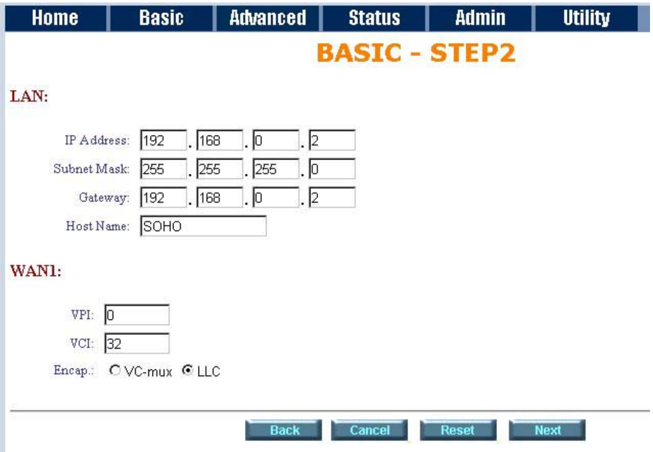
Click Bridge and CPE Side to setup Bridge mode of the Router and then click Next.



BASIC - STEP1

Operation Mode:

System Mode: ○ ROUTE ● BRIDGE
SHDSL Mode: ○ CO Side ● CPE Side



BASIC - STEP2

LAN:

IP Address: 192 . 168 . 0 . 2
Subnet Mask: 255 . 255 . 255 . 0
Gateway: 192 . 168 . 0 . 2
Host Name: SOHO

WAN1:

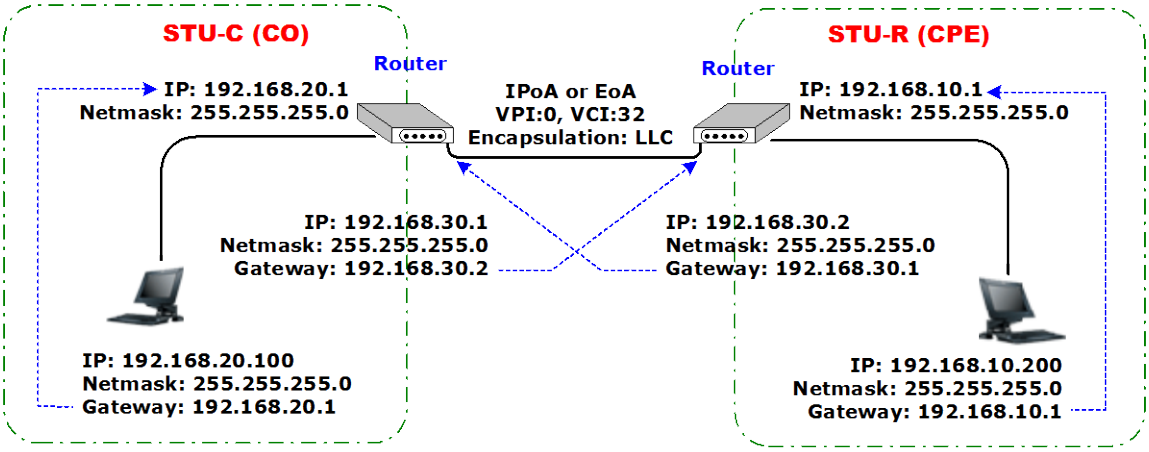
VPI: 0
VCI: 32
Encap.: ○ VC-mux ● LLC

Enter **LAN** Parameters
IP: 192.168.0.2
Subnet Mask: 255.255.255.0
Gateway: 192.168.0.2
Host Name: SOHO

Enter **WAN1** Parameters
VPI: 0
VCI: 32
Click LLC
Click Next

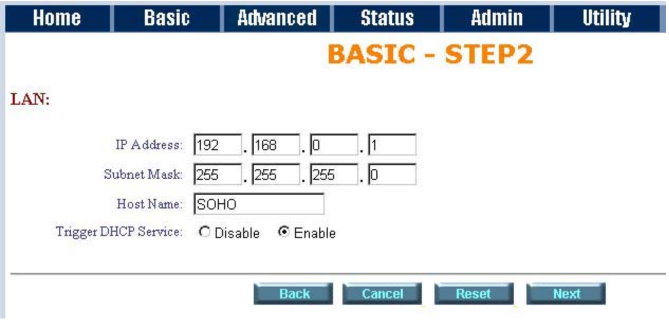
The screen will prompt the new configured parameters. Check the parameters and Click Restart The router will reboot with the new setting.

4.6.2 LAN to LAN connection with routing mode



4.6.2.1 CO Side

Click ROUTE and CO Side to setup Routing mode of the Router and then click Next



IP Address: 192 . 168 . 0 . 1
Subnet Mask: 255 . 255 . 255 . 0
Host Name: SOHO
Trigger DHCP Service: ○ Disable ● Enable

Type **LAN** parameters:

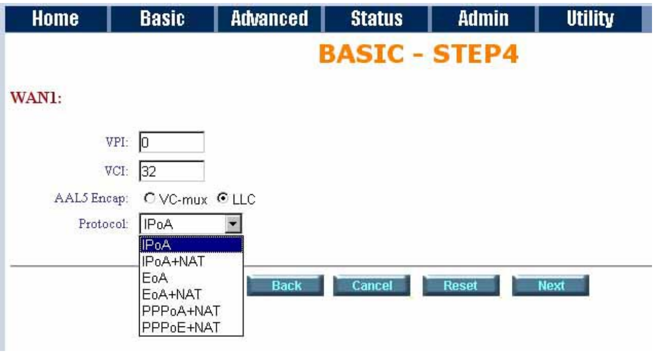
IP Address: 192.168.20.1

Subnet Mask: 255.255.255.0

Host Name: SOHO

DHCP Service: Disable or Enable

For more **DHCP** service, review the chapter on DHCP Service



VPI: 0
VCI: 32
AAL5 Encap: ○ VC-mux ● LLC
Protocol: IPoA

Type the **WAN1** Parameters;

VPI: 0

VCI: 32

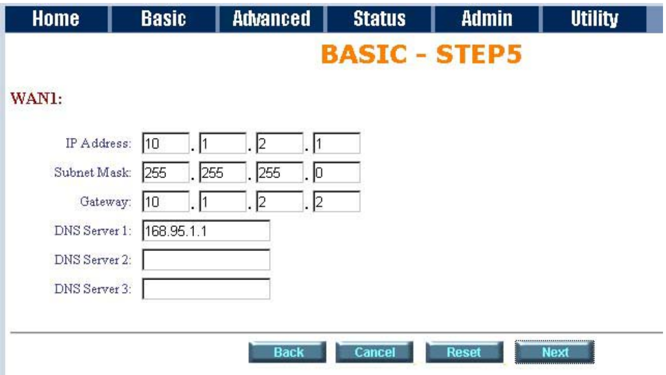
AAL5 Encap: LLC

Protocol: IPoA , EoA , IPoA + NAT or EoA + NAT

Note: The Protocol used in CO and CPE have to be the same.

Click Next to setup the IP parameters.

For more understanding about **NAT,** review the chapter of NAT/DMZ .



BASIC - STEP5

WAN1:

IP Address: 10 . 1 . 2 . 1

Subnet Mask: 255 . 255 . 255 . 0

Gateway: 10 . 1 . 2 . 2

DNS Server 1: 168.95.1.1

DNS Server 2:

DNS Server 3:

IP Address: 192.168.20.1

Subnet Mask: 255.255.255.0

Gateway: 192.169.30.2

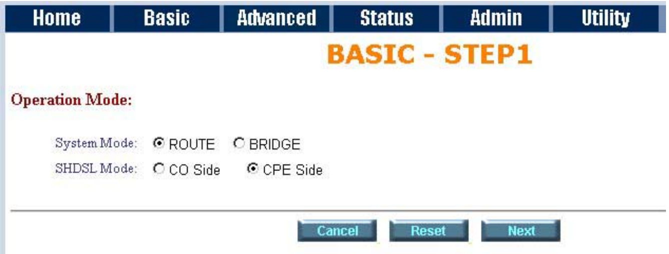
Click Next

The screen will prompt the parameters that we will write in NVRAM. Check the parameters before writing in NVRAM.

Press Restart to restart the router working with new parameters or press continue to setup another parameter.

4.6.2.2 CPE side

Click ROUTE and CPE Side then press Next.

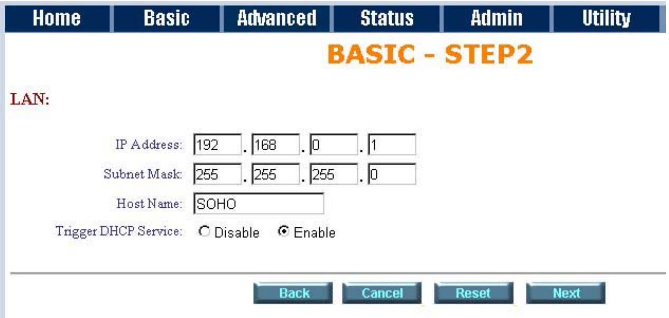


BASIC - STEP1

Operation Mode:

System Mode: ● ROUTE ○ BRIDGE

SHDSL Mode: ○ CO Side ● CPE Side



BASIC - STEP2

LAN:

IP Address: 192 . 168 . 0 . 1
Subnet Mask: 255 . 255 . 255 . 0
Host Name: SOHO
Trigger DHCP Service: ○ Disable ● Enable

Type LAN parameters:

IP Address: 192.168.10.1

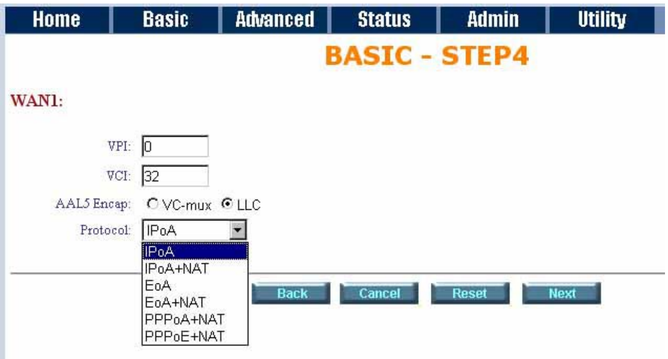
Subnet Mask: 255.255.255.0

Host Name: SOHO

DHCP Service: Disable or Enable

For more **DHCP** service, review the chapter of DHCP Service.

Type the WAN1 Parameters:



BASIC - STEP4

WAN1:

VPI: 0
VCI: 32
AAL5 Encap: ○ VC-mux ● LLC
Protocol: IPoA

VPI: 0

VCI: 32

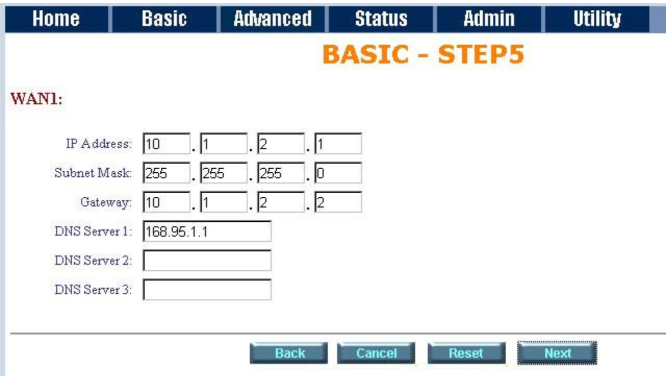
AAL5 Encap: LLC

Protocol: IPoA , EoA , IPoA + NAT or EoA + NAT

Note: The Protocol used in CO and CPE have to be the same.

Click Next to setup the IP parameters.

For more understanding about **NAT**, review the chapter of NAT/DMZ.



BASIC - STEP5

WAN1:

IP Address: 10 . 1 . 2 . 1
Subnet Mask: 255 . 255 . 255 . 0
Gateway: 10 . 1 . 2 . 2
DNS Server 1: 168.95.1.1
DNS Server 2:
DNS Server 3:

IP Address: 192.168.30.2

Subnet mask: 255.255.255.0

Gateway: 192.169.30.1

Click Next

The screen will prompt the parameters that we will write in NVRAM. Check the parameters before writing in NVRAM.

Press Restart to restart the router working with new parameters or press continue to setup another parameter.

5 Configuration via Serial Console or Telnet with Manu Driven Interface

In this section, the detail of menu-driven user interface will be described on below.

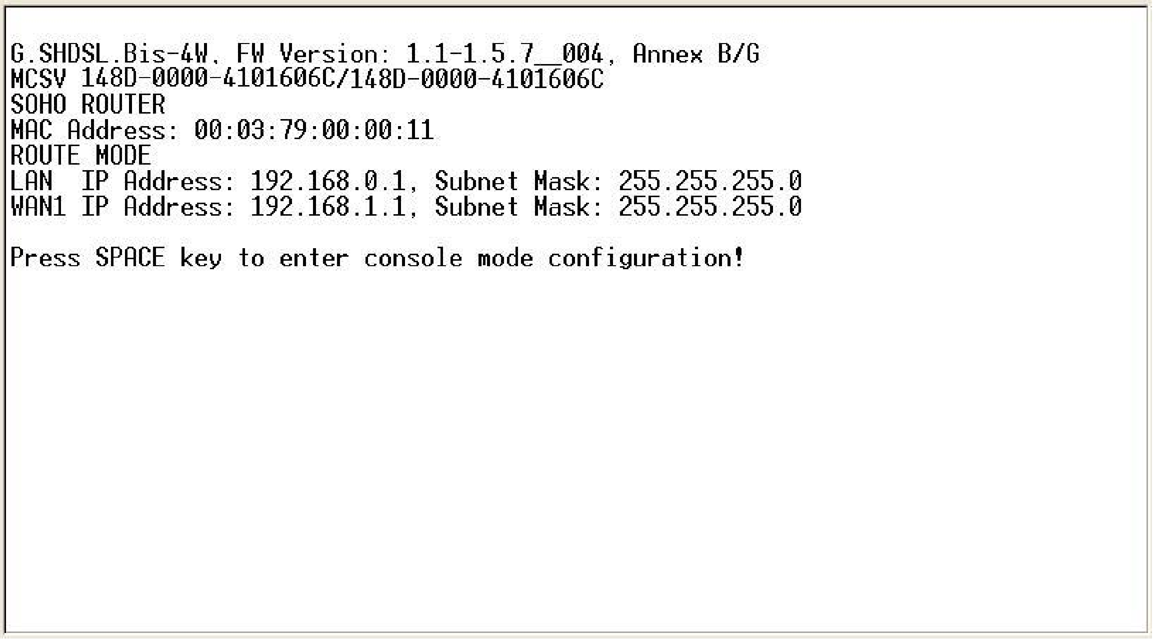
5.1 Introduction

5.1.1 Serial Console

Check the connectivity of the RS-232 cable. Connect the male 9-pin end of console port of the router and connect the female end to a serial port of your computer.
Start your terminal access program by VT100 terminal emulation with the following parameters:

Parameter	Value
Baudrate	9600bps
Data Bits	8
Parity Check	No
Stop Bits	1
Flow-control	No

Press the SPACE key until the login screen appears. When you see the login screen, you can logon to Router.



```
G.SHDSL.Bis-4W, FW Version: 1.1-1.5.7__004, Annex B/G
MCSV 148D-0000-4101606C/148D-0000-4101606C
SOHO ROUTER
MAC Address: 00:03:79:00:00:11
ROUTE MODE
LAN  IP Address: 192.168.0.1, Subnet Mask: 255.255.255.0
WAN1 IP Address: 192.168.1.1, Subnet Mask: 255.255.255.0

Press SPACE key to enter console mode configuration!
```

Note: Only SPACE key invoke the login prompt. Pressing other keys does not work.

```
User: admin
Password: *****
```

Note: The factory default **User** and **Password** are “admin” both.

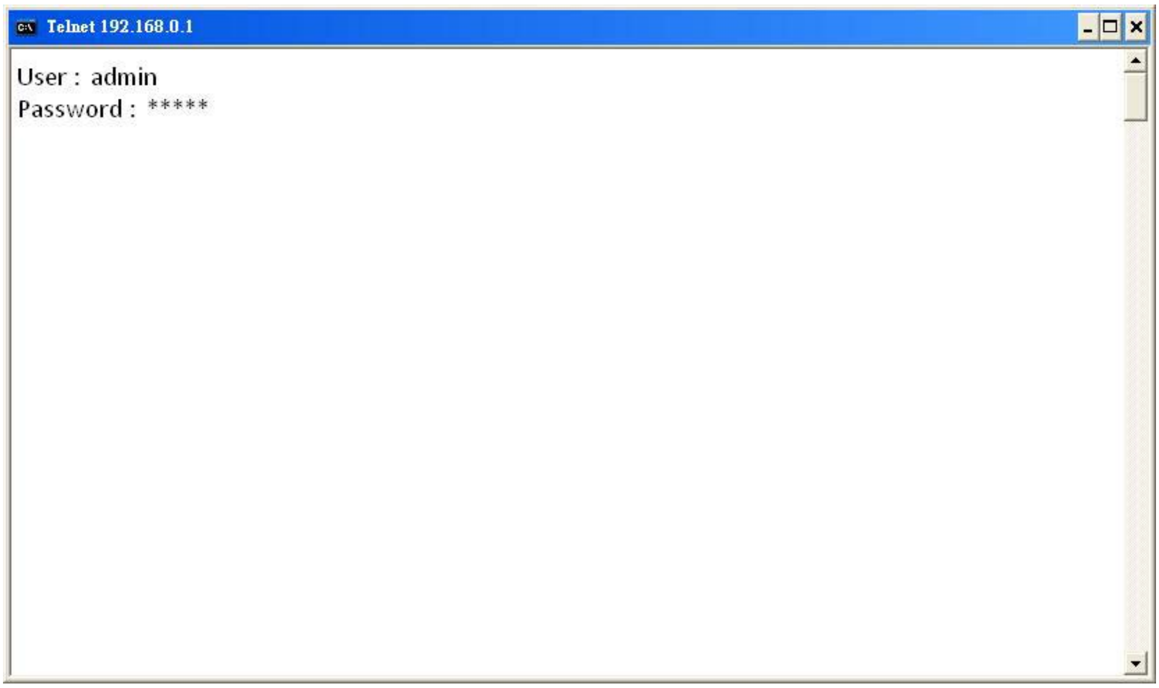
```
User: admin
Password: *****
```

5.1.2 Telnet

Make sure the correct Ethernet cable connected the LAN port of your computer to this Router. The LAN LNK LED indicator on the front panel shall light if a correct cable is used. Starting your Telnet client with VT100 terminal emulation and connecting to the management IP of Router, wait for the login prompt appears. Input User and Password after login screen pop up,

```
User: admin
Password: *****
```

Note: The default IP address is 192.168.0.1.



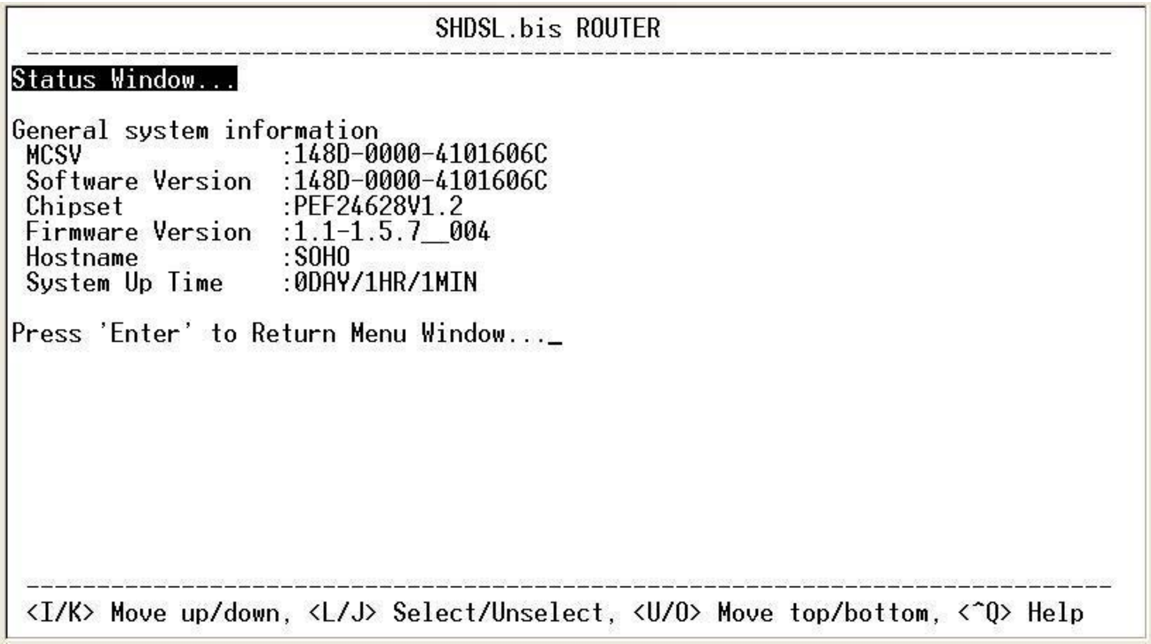
```
User : admin
Password : *****
```

5.1.3 Operation Interface

For serial console and Telnet management, the Router implements two operational interfaces: Command Line Interface (CLI) and menu driven interface. The CLI mode provides users a simple interface, which is better for working with script file. The menu driven interface is a user-friendly interface to general operations. The command syntax for CLI is the same as that of the menu driven interface. The only difference is that the menu driven interface shows you all of available commands for you to select. You don't need to remember the command syntax and save your time on typing the whole command line.

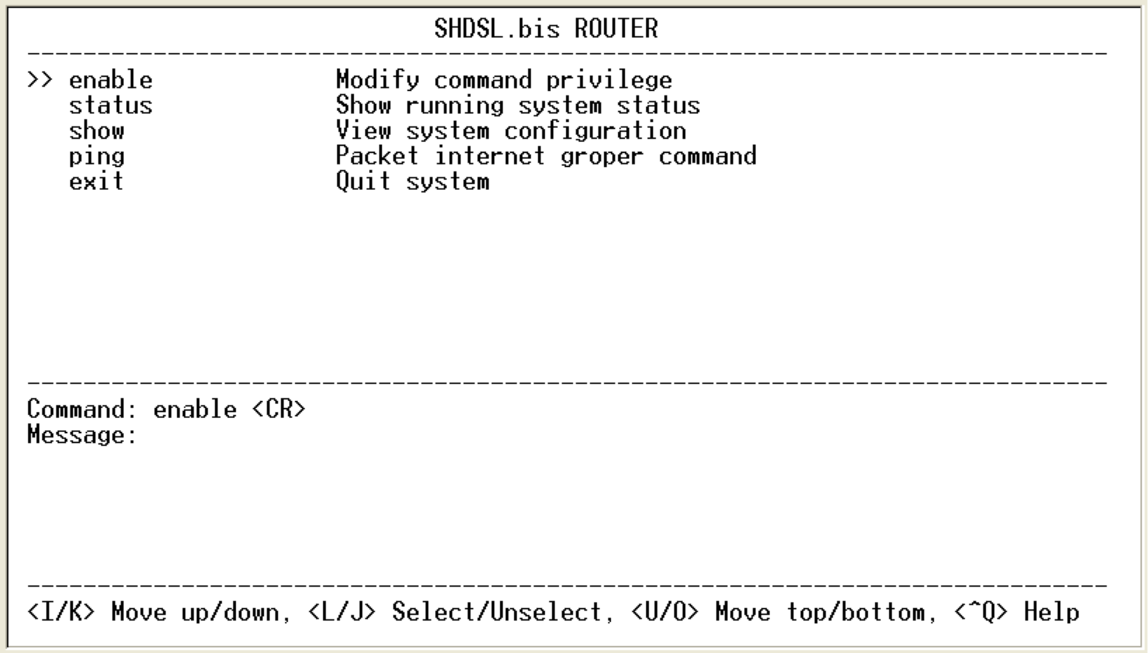
The following figure gives you an example of the menu driven interface. In the menu, you scroll up/down by pressing key **I / K**, select one command by key **L**, and go back to a higher level of menu by key **J**.

For example, to show the system information, just logon to the Router, move down the cursor by pressing key **K** twice and select "show" command by key L, you shall see a submenu and select "system" command in this submenu, then the system will show you the general information.



```
                              SHDSL.bis ROUTER
 ----------------------------------------------------------------------------
Status Window...

General system information
 MCSV                 :148D-0000-4101606C
 Software Version     :148D-0000-4101606C
 Chipset              :PEF24628V1.2
 Firmware Version     :1.1-1.5.7__004
 Hostname             :SOHO
 System Up Time       :0DAY/1HR/1MIN

Press 'Enter' to Return Menu Window..._









 ----------------------------------------------------------------------------
 <I/K> Move up/down, <L/J> Select/Unselect, <U/O> Move top/bottom, <^Q> Help
```

5.1.4 Window structure



```
                              SHDSL.bis ROUTER
-----------------------------------------------------------------------------
>> enable                 Modify command privilege
   status                 Show running system status
   show                   View system configuration
   ping                   Packet internet groper command
   exit                   Quit system








-----------------------------------------------------------------------------
Command: enable <CR>
Message:






-----------------------------------------------------------------------------
<I/K> Move up/down, <L/J> Select/Unselect, <U/O> Move top/bottom, <^Q> Help
```

From top to bottom, the window is divided into four parts:

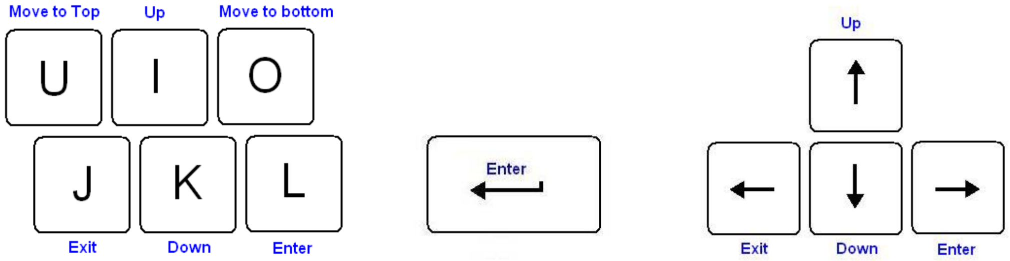
1. **Product name**: "SHDSL.bis ROUTER"
2. **Menu field**: Menu tree prompts on this field. Symbol "**>>**" indicates the cursor place.
3. **Configuring field**: You will configure the parameters in this field. **< parameters >** indicates the parameters you can choose and **< more…>** indicates that there have submenu in the title.
4. Operation command for help

The following table shows the parameters in the brackets.

Command	Description
<ip>	An item enclosed in brackets is required. If the item is shown in lower case bold, it represents an object with special format. For example, **<ip>** may be **192.168.0.3**.
<Route|Bridge>	Two or more items enclosed in brackets and separated by vertical bars means that you must choose exactly one of the items. If the item is shown in lower case bold with leading capital letter, it is a command parameter. For example, **Route** is a command parameter in **<Route|Bridge>**.
[1~1999]	An item enclosed in brackets is optional.
[1~65534|-t]	Two or more items enclosed in brackets and separated by vertical bars means that you can choose one or none of the items.

5.1.5 Menu Driven Interface Commands

Before changing the configuration, familiarize yourself with the operations list in the following table. The operation list will be shown on the window.



Menu Driven Interface Commands

Keystroke	Description
[UP] or I	Move to above field in the same level menu.
[DOWN] or K	Move to below field in the same level menu.
U	Move to top field in the same level menu
O	Move to bottom field in the same level menu
[LEFT] or J	Move back to previous menu
[RIGHT], L or [ENTER]	Move forward to submenu
[TAB]	To choose another parameters
Ctrl + C	To quit the configuring item
Ctrl + D	Disconnection
Ctrl + U	Hot-key switch to command line interface
Ctrl + Q	Display help menu

5.2 Main menu before enable

When enter to menu on the following. All of the configuration commands are placed in the subdirectories of Enable protected by supervisor password. On the other hand, unauthorized user cannot change any configurations but viewing the status and configuration of the router and using ping command to make sure the router is working.

```
-------------------------------------------------------------------------
>>  enable      Modify command privilege
    status      Show running system status
    show        View system configuration
    ping        Packet internet groper command
    exit        Quit system

-------------------------------------------------------------------------
```

If you need setup and manage the router, you must set **enable** command before.

5.3 Enable

To setup the router, move the cursor " >>" to **enable** and press **enter** key. While the screen appears, type the supervisor password. The default supervisor password is ***root***. The password will be prompted as " * " symbol for system security.

```
----------------------------------------------------------------------
Command: enable <CR>
Message: Please input the following information.

Supervisor password: ****
----------------------------------------------------------------------
```

In this sub menu, you can setup management features and upgrade software, backup the system configuration and restore the system configuration via utility tools.

For any changes of configuration, you have to write the new configuration to NVRAM and reboot the router to work with new setting.

The screen will prompt as follow:

```
-------------------------------------------------------------------------------
>> enable          Modify command privilege
   setup           Configure system
   status          Show running system status
   show            View system configuration
   write           Update flash configuration
   reboot          Reset and boot system
   ping            Packet internet groper command
   admin           Setup management features
   utility         TFTP upgrade utility
   exit            Quit system

-------------------------------------------------------------------------------
```

Command Description:

Command	Description
enable	Modify command privilege. When you login via serial console or Telnet, the router defaults to a program execution (read-only) privileges to you. To change the configuration and write changes to nonvolatile RAM (NVRAM), you must work in enable mode.
setup	To configure the router, you have to use the setup command.
status	View the status of router.
show	Show the system and configuration of router.
write	Update flash configuration. After you have completed all necessary setting, make sure to write the new configuration to NVRAM by "**write**" command and reboot the system, or all of your changes will not take effect.
reboot	Reset and boot system. After you have completed all necessary setting, make sure to write the new configuration to NVRAM and reboot the system, otherwise, all of your changes will not take effect.
ping	Internet ping command.
admin	You can setup management features in this command.

utility	Upgrade software and backup and restore configuration.
exit	Quit system.

5.4 Status

You can view running system status of SHDSL.bis, WAN, route, interface, fireware, ip_qos and stp via **status** command.

Move cursor “ **>>** “ to **status** and press enter.

```
-------------------------------------------------------------------------------
>> shdsl.bis       Show SHDSL.bis status
   wan             Show WAN interface status
   route           Show routing table
   interface       Show interface statistics status
   firewall        Show firewall status
   ip_qos          Show IP QoS statistics
   stp             Show STP status
   clear           Reset statistics`

-------------------------------------------------------------------------------
```

Command	Description
shdsl.bis	The SHDSL.bis status includes line rate, SNR margin, TX power, attenuation, and CRC error of the product, and SNR margin, attenuation and CRC error of remote side. The router can access remote side’s information via EOC (embedded operation channel).
wan	WAN status shows all their parameters including IP address ,Net mask, PVC and protocol information
route	You can see the routing table via route command.
interface	The statistic status of WAN and LAN interface can be monitor by interface command.
firewall	Show firewall status (for firewall models only)
Ip_qos	Show IP QOS status
stp	Show the STP status on all LANs and WANs
clear	Clear all statistics data

5.4.1 Shdsl.bis

Move cursor “ **>>** “ to **shdsl.bis** and press enter.

If the Router is four wires model, there will show two channel’s status as the following:

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Monitoring Window...
<SHDSL.bis Status>
```

```
Channel                    :   A      /     B
SHDSL.bis Mode             : CPE Side / CPE Side
Line Rate(n*64)            :   0kbps   /    0kbps
Current SNR Margin         :   0dB    /    0dB
Attenuation                :   0dB    /    0dB
CRC Error Count            :   0      /     0

SHDSL Remote Side Status
Channel                    :   A      /     B
Current SNR Margin         :   0dB    /    0dB
Attenuation                :   0dB    /    0dB
CRC Error Count            :   0      /     0

 -----------------------------------------------------------------------------
```

If the Router is two wires model, there will show one channel's status as the following:

```
-----------------------------------------------------------------------------
Monitoring Window...
<SHDSL.bis Status>
SHDSL.bis Mode
Line Rate(n*64)            :CPE Side
Current SNR Margin         :0kbps
Attenuation                :0dB
CRC Error Count            :0dB
                           :0
SHDSL Remote Side Status
Current SNR Margin         :0dB
Attenuation                :0dB
CRC Error Count            :0

 -----------------------------------------------------------------------------
```

Show SHDSL.bis status includes the Mode, Line Rate, Current SNR Margin, Attenuation and CRC error count on both side. There are real time status, the screen will be refresh any time.
You can press the "c" key to clear CRC error counter. Press Ctrl-C can quit this screen.

5.4.2 Wan

Move cursor " **>>** " to **wan** and press enter.

```
------------------------------------------------------------------------
Monitoring Window...
 WAN    IP address   /    NetMask     VPI/ VCI  Encap  Protocol Active
----- --------------- --------------- --- ----- ------ -------- ------
WAN1  192.168.  1.  1/255.255.255.  0   0/   32  LLC      IPoA     No
WAN2  192.168.  2.  1/255.255.255.  0   0/   34  LLC   Ethernet    No
WAN3  192.168.  3.  1/255.255.255.  0   0/   34  LLC   Ethernet    No
WAN4  192.168.  4.  1/255.255.255.  0   0/   35  LLC      IPoA     No
WAN5  192.168.  5.  1/255.255.255.  0   0/   36  LLC     PPPoA     No
WAN6  192.168.  6.  1/255.255.255.  0   0/   37  LLC   Ethernet    No
WAN7  192.168.  7.  1/255.255.255.  0   0/   38  LLC   Ethernet    No
WAN8  192.168.  8.  1/255.255.255.  0   0/   39  LLC   Ethernet    No
 ------------------------------------------------------------------------
```

Show WAN status include IP address, Net Mask, VPI/VCI, encapsulation type, protocol on each

WAN ports

5.4.3 Route

Move cursor “ **>>** “ to **Route** and press enter.

```
------------------------------------------------------------------------
Monitoring Window...
Flag   Destination   /     Netmask   /    Gateway       Interface     Portname
---- ------------------------------------------------ ----------- -------
 C       192.168.0.0/  255.255.255.0/    directly      192.168.0.1      LAN
 C         127.0.0.1/255.255.255.255/    directly        127.0.0.1 Loopback

------------------------------------------------------------------------
```

You can view the routing table on here.

5.4.4 Interface

Move cursor “ **>>** “ to **Interface** and press enter.

```
----------------------------------------------------------------------------
Monitoring Window...
<Interface Statistics>
Port    InOctets    InPackets   OutOctets   OutPackets InDiscards OutDiscards
---- ------------- ---------- ------------- ---------- ---------- -----------
 LAN             0          0         512          8          0          0
WAN1             0          0           0          0          0          0
WAN2             0          0           0          0          0          0
WAN3             0          0           0          0          0          0
WAN4             0          0           0          0          0          0
WAN5             0          0           0          0          0          0
WAN6             0          0           0          0          0          0
WAN7             0          0           0          0          0          0
WAN8             0          0           0          0          0          0

-----------------------------------------------------------------------------
```

You can view interface statistics data on one LAN port and maximum eight WAN ports.

5.4.5 firewall

Move cursor “ **>>** “ to **firewall** and press enter.

```
-----------------------------------------------------------------------------
Monitoring Window...

<Current Firewall Status>
      Attack Type     Current Status History Status
---------------------- ------------- -------------
      All DoS protects are disabled!
---------------------- ------------- -------------
```

```
Packets dropped by DoS protect function: 0
Packets dropped by SPI filter function: 0
Packets dropped by packet filter function: 0
-----------------------------------------------------------------------------
```

You can view firewall statistics. (Only for firewall models.)

5.4.6 ip_qos

Move cursor “ **>>** “ to **Ip_qos** and press enter.

```
-----------------------------------------------------------------------------
 Command: status ip_qos <0~8>
 Message: Please input the following information.

 Interface number <0~8>:

-----------------------------------------------------------------------------
```

You can view IP QoS statistics data on one LAN port.

```
-----------------------------------------------------------------------------
Monitoring Window...

<Current IP QoS Statistics - LAN Interface>
Preced.   InBytes  InPackets   OutBytes OutPackets OutDropByts OutDropPkts
------- ---------- ---------- ---------- ---------- ----------- -----------
  0          0         0         0         0          0          0
  1          0         0         0         0          0          0
  2          0         0         0         0          0          0
  3          0         0         0         0          0          0
  4          0         0         0         0          0          0
  5          0         0         0         0          0          0

-----------------------------------------------------------------------------
```

5.4.7 STP

Move cursor “ **>>** “ to **STP** and press enter.

```
-----------------------------------------------------------------------------
<STP Status>
Bridge ID / Designated ROOT ID  : 8000-000379-572002 / 8000-000379-572002
ROOT Port / ROOT Path Cost     : None /     0
Max Age/Forward Delay/Hello Time:  20 /   15 /    2(secs)
             LAN    WAN1   WAN2   WAN3   WAN4   WAN5   WAN6   WAN7   WAN8
 ----------  ----   ----   ----   ----   ----   ----   ----   ----   ----
      State  F      D      D      D      D      D      D      D      D
   Priority  128    128    128    128    128    128    128    128    128
  Path Cost  100    500    500    500    500    500    500    500    500

<Hint> D-Disable, B-Blocking, LS-Listening, LN-Learning, F-Forwarding.
-----------------------------------------------------------------------------
```

You can view all STP status on all LAN and WANs ports.

The STP state per LANs and WANs are as following:

Blocking - A port that would cause a switching loop, no user data is sent or received but it may go into forwarding mode if the other links in use were to fail and the spanning tree algorithm determines the port may transition to the forwarding state. BPDU data is still received in blocking state.

Listening - The switch processes BPDUs and awaits possible new information that would cause it to return to the blocking state.

Learning - While the port does not yet forward frames (packets) it does learn source addresses from frames received and adds them to the filtering database (switching database)

Forwarding - A port receiving and sending data, normal operation. STP still monitors incoming BPDUs that would indicate it should return to the blocking state to prevent a loop.

Disabled - Not strictly part of STP, a network administrator can manually disable a port.

5.4.8 Clear

Move cursor “ **>>** “ to **Clear** and press enter.
You can clear all statistics by this command.

```
-----------------------------------------------------------------------------
Command: status clear <CR>
 Message: Clear OK!

 -----------------------------------------------------------------------------
```

5.5 Show

You can view the system information, configuration, and configuration in command script by **show** command.

Move cursor “ **>>** “ to **show** and press enter.

```
--------------------------------------------------------------------------------------------
>> system          Show general information
   config          Show all configuration
   script          Show all configuration in command script

--------------------------------------------------------------------------------------------
```

Command	Description
system	The general information of the system will show in system command.
config	Config command can display detail configuration information.
script	Configuration information will prompt in command script.

5.5.1 System information

Move cursor to “ **>>** “ to **system** and press enter.

```
---------------------------------------------------------------------------
Status Window...

General system information
 MCSV                :148D-0000-4101606C
 Software Version    :148D-0000-4101606C
 Chipset             :PEF24628V1.2
 Firmware Version    :1.1-1.5.7__004
 Hostname            :SOHO
 System Up Time      :0DAY/2HR/53MIN

---------------------------------------------------------------------------
```

From this screen, you can know more about the general information of this router.

5.5.2 Configuration information

Move cursor to “ **>>** “ to **config** and press enter.
You can view all setting using table format.

5.5.3 Configuration with Script format

Move cursor to “ **>>** “ to **script** and press enter.
You can view all setting using script format.

5.6 Write

For any changes of configuration, you must write the new configuration to NVRAM using **write** command and reboot the router to take affect.

Move cursor to “ **>>** “ to **write** and press enter.

```
----------------------------------------------------------------------
Command: write <CR>
Message: Please input the following information.

Are you sure? (y/n): y
----------------------------------------------------------------------
```

Press “y” to confirm the write operation.

5.7 Reboot

To reboot the router, please use “**reboot**” command. Move cursor to “ **>>** “ to **reboot** and press enter.

```
----------------------------------------------------------------------
Command: reboot <CR>
Message: Please input the following information.

Do you want to reboot? (y/n): y
----------------------------------------------------------------------
```

Press “y” to confirm the reboot operation.

5.8 Ping

Ping command will be used to test the Ethernet connection of router or Internet linking condition. Move cursor “ **>>** “ to **ping** and press enter.

```
----------------------------------------------------------------------
Command: ping <ip> [1~65534|-t] [1~1999]
Message: Please input the following information.

IP address <IP> : 10.0.0.1
Number of ping request packets to send (TAB select): -t
Data size [1~1999]: 32
----------------------------------------------------------------------
```

There are 3 parameters for ping command:

`<ip> [1~65534|-t] [1~1999]`

IP address: The IP address which you want to ping.

Number of ping request packed to send, key TAB for further selection:

- Default: It will send 4 packets only
- 1~65534: Set the number of ping request packets from 1 to 65534
- -t : It will continuous until you key Ctrl+C to stop

Data Size: From 1 to 1999

5.9 Administration

You can modify the user profile, security, SNMP (Sample Network Management Protocol), supervisor information and SNTP (Simple Network Time Protocol) in **admin**.

For configuration the parameters, move the cursor “ **>>** “ to **admin** and press enter.

```
---------------------------------------------------------------------------------------------
>> user              Manage user profile
   security          Setup system security
   snmp              Configure SNMP parameter
   passwd            Change supervisor password
   id                Change supervisor ID
   sntp              Configure time synchronization

   ------------------------------------------------------------------------------------------
```

5.9.1 User Profile

You can use **user** command to clear, modify and list the user profile. You can setup at most five users to access the router via console port or telnet in user profile table however users who have the supervisor password can change the configuration of the router. Move the cursor " **>>** " to **user** and press enter key.

```
---------------------------------------------------------------------------------------------
>> clear             Clear user profile
   modify            Modify the user profile
   list              List the user profile

---------------------------------------------------------------------------------------------
```

You can delete the user by number using **clear** command. If you do not make sure the number of user, you can use **list** command to check it. **Modify** command is to modify an old user information or add a new user to user profile.

To modify or add a new user, move the cursor to **modify** and press enter.

```
----------------------------------------------------------------------
Command: admin user modify <1~5> <more...>
Message: Please input the following information.

Legal access user profile number <1~5> : 2
----------------------------------------------------------------------
```

The screen will prompt as follow.

```
---------------------------------------------------------------------------------------------
>> Attrib            UI mode
   Profile           User name and password

---------------------------------------------------------------------------------------------
```

There are two UI mode, **command** and **menu** mode, to setup the router. We will not discuss command mode in this manual.

Move the cursor to **Attrib** to change the UI mode on this profile

Move the cursor to **Profile** and press enter, you can change the username and their password on this profile.

The screen will prompt as follow:

```
------------------------------------------------------------------------
 Command: admin user modify 5 profile <name> <pass_conf>
 Message: Please input the following information.

 Legal user name (ENTER for default) <admin>: superman
 Input the old Access password: ****
 Input the new Access password: ****
 Re-type Access password: ****
 ------------------------------------------------------------------------
```

For example, set up the legal user name is “superman” and access password is”1234”,and use write command to store on NVRAM.

Finally, you can use **list** command to check the listing of five profiles including on user name and their UI mode. On next time you re-enter this system, you can use this set of username and password. You can set up maximum to five profiles such that five sets of username and their password.

```
User: superman
Password: ****
```

User Profile

User profile	User name	Password	Attrib
1			□Menu □Command
2			□Menu □Command
3			□Menu □Command
4			□Menu □Command
5			□Menu □Command

For example, when using the command **list**, the screen will prompt as follow:

```
------------------------------------------------------------------------
Legal Access User Profile
  No     User  Name         UI Mode
 ---- ------------------ -----------
   1            test        Menu
   2          test-1        Menu
   3          test-2      Command
   4          test-3      Command
   5         superman       Menu

------------------------------------------------------------------------
```

5.9.2 Security

Security command can be configured sixteen legal IP address for telnet access and telnet port number.

Move the cursor “ **>>** “ to **security** and press enter.

```
>> port              Configure telnet TCP port
   ip_pool           Legal client IP address pool
   list              Show security profile

```

Telnet TCP Port:

Telnet TCP Port	

Legal client IP Address pool:

	Legal client IP Address pool
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	

Move the cursor to **port** and press enter. You can setup port number form 1 to 65534.

Move the cursor to **IP Pool** and press enter, there are sixteen legal IP address for telnet access. The default legal address is 0.0.0.0. It means that there is no restriction of IP to access the router via telnet. There have two sub-menu: **modify** and **clear** for easy to set up each one.

Move the cursor to **list** and press enter, you can view full listing on security profile including the Telnet listing TCP port and 16 host IP address.

5.9.3 SNMP

Simple Network Management Protocol (SNMP) is the protocol not only governing network management, but also the monitoring of network devices and their functions.

The router can generate SNMP traps to indicate alarm conditions, and it relies on SNMP community strings to implement SNMP security. This router support MIB I & II.

Move the cursor " **>>** " to **snmp** and press enter.

```
--------------------------------------------------------------------------------
>> community       Configure community parameter
   trap            Configure trap host parameter

--------------------------------------------------------------------------------
```

5.9.4 Community

There are 5 entries of SNMP community can be configured in this system.

Move the cursor to **community** and press enter.

```
-----------------------------------------------------------------------------
Command: admin snmp community <1~5> <more...>
Message: Please input the following information.

Community entry number <1~5> : 2
-----------------------------------------------------------------------------
```

The screen will prompt as follow:

```
------------------------------------------------------------------------------
>> edit            Edit community entry
   list            Show community configuration

------------------------------------------------------------------------------
```

Move the cursor to **edit** and press enter. You can setup the following:

Validate : Set **Enable** or **Disable**
Community : Key in the string
Access right : Set **Read only**, **Read Write** or **Denied**

Move the cursor to **list** and press enter, you can view full listing on SNMP Community Pool. 5 entries of SNMP trap are allowed to be configured in this system.

SNMP Community:

SNMP entry(1~5)	
Validate	□Enable □Disable
Community	
Access Right :	□Read only □Read Write □Denied

5.9.4.1 Trap Host

Move the cursor to **trap** and press enter.

```
---------------------------------------------------------------------
Command: admin snmp trap <1~5> <more...>
Message: Please input the following information.

Trap host entry number <1~5> : 2
---------------------------------------------------------------------
```

The screen will prompt as follow:

```
------------------------------------------------------------------------------
>> edit            Edit trap host parameter
   list            Show trap configuration

------------------------------------------------------------------------------
```

Move the cursor to **edit** and press enter, you can setup the following:

Version : **Disable**, **1** or **2**
Trap host IP address : Key in the IP address
Community : Key in the string

SNMP Trap Host:

Trap Host entry(1~5)	
Version	□Disable □Ver.1 □Ver.2
IP Address	
Community	

Move the cursor to **list** and press enter, you can view full listing on SNMP Trap Host Pool.

5.9.5 Supervisor Password and ID

The supervisor password and ID is the last door for security but the most important. Users who access the router via web browser have to use the ID and password to configure the router and users who access the router via telnet or console mode have to use the password to configure the router. Suggest to change the ID and password after the first time of configuration, and save it. At next time when you access to the router, you have to use the new password.

	Factory default
User name	admin
Password	admin
Supervisor ID	root
Supervisor Password	root

```
----------------------------------------------------------------------
Command: admin passwd <pass_conf>
Message: Please input the following information.

Input old Supervisor password: ****
Input new Supervisor password: ********
Re-type Supervisor password: ********
----------------------------------------------------------------------
```

The default supervisor password is “root”.

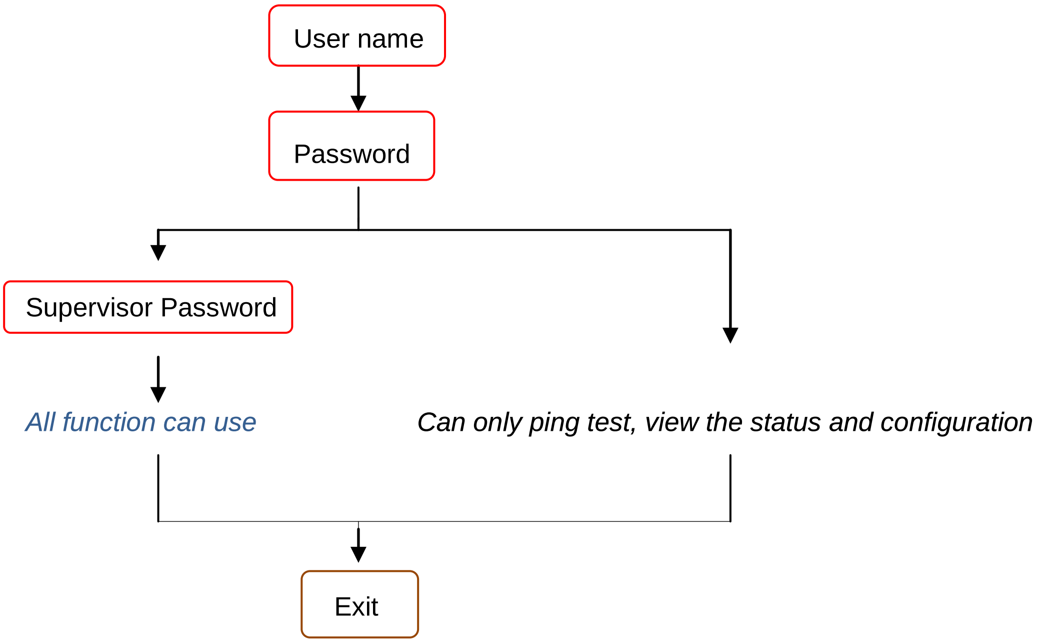
```
----------------------------------------------------------------------
Command: admin id <pass_conf>
Message: Please input the following information.

Legal user name (Enter for default) <root> : test
----------------------------------------------------------------------
```

The default admin ID is “root”.

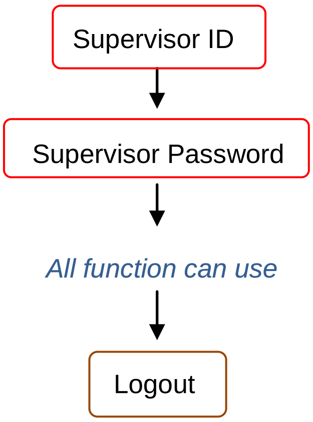
Supervisor ID and Password:

Supervisor ID	
Supervisor Password	

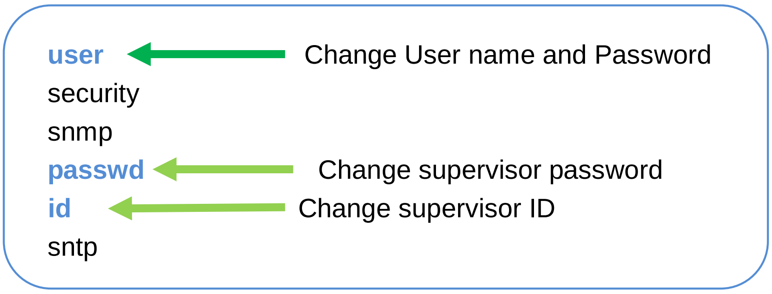
Telnet Console mode:



Web Brower mode:



Administration:



5.9.6 SNTP

Time synchronization is an essential element for any business that relies on an IT system. The reason for this is that these systems all have clocks, which are the source of time for files or operations they handle. Without time synchronization, time on these systems varies with each other or with the correct time and this can cause- virtual server schedule processes to fail and system log exposures with wrong data.

There are two methods to synchronize time, **synchronize with PC** or **SNTPv4**. If you choose synchronize with PC, the router will synchronize with PC's internal timer. If you choose SNTPv4, the router will use the protocol to synchronize with the time server. For synchronization the time server with SNTP v4, needs to configure service, **time_server** and **time_zone**. For synchronization with PC, doesn't need to configure the above parameters.

Move the cursor " **>>** " to **sntp** and press enter.

```
-------------------------------------------------------------------------------------------------
>> method          Select time synchronization method
   service         Trigger SNTP v4.0 service
   time_server1    Configure time server 1
   time_server2    Configure time server 2
   time_server3    Configure time server 3
   Update_rate     Configure update period
   time_zone       Configure GMT time zone offset
   list            Show SNTP configuration

-------------------------------------------------------------------------------------------------
```

To configure SNTP v4 time synchronization protocol, follow the below procedures:

move the cursor to **method** and press enter.

```
----------------------------------------------------------------------
Command: admin sntp method <SNTPv4|SyncWithPC>
Message: Please input the following information.

SYNC method (Enter for default) <SyncWithPC> : SNTPv4
----------------------------------------------------------------------
```

Move the cursor to **service** and press enter.

```
----------------------------------------------------------------------
Command: admin sntp service <Disable|Enable>
Message: Please input the following information.

Active SNTP v4.0 service (Tab Select) <Enable> : Enable
----------------------------------------------------------------------
```

Move the cursor to **time_server1** and press enter.

```
----------------------------------------------------------------------
Command: admin sntp time_server1 <string>
Message: Please input the following information.

Time server address(Enter for default) <ntp-2.vt.edu> : ntp-2.vt.edu
----------------------------------------------------------------------
```

You can configure three time servers in this system with time_server1, time_server2 and time_server3.

The default time servers are the following:

- time_server1 : ntp-2.vt.edu
- time_server2 : ntp.drydog.com
- time_server3 : ntp1.cs.wisc.edu

Move the cursor to **update_rate** and press enter.

```
----------------------------------------------------------------------
Command: admin sntp update_rate <10~268435455>
Message: Please input the following information.

Update period (secs) (Enter for default) <3600> : 86400
----------------------------------------------------------------------
```

Move the cursor to **time_zone** and configure where your router is placed. The easiest way to know the time zone offset hour is from your PC clock. Double click the clock at the right corner of monitor and check the time zone of your country. There will have a (GMT+XX:XX) or (GMT-XX.XX) information.

```
----------------------------------------------------------------------
Command: admin sntp time_zone <-12~12>
Message: Please input the following information.

GMT time zone offset (hours) (Enter for default) : -8
----------------------------------------------------------------------
```

Time synchronization:

Method	□Sync with PC □SNTP V4.0
SNTP V4.0 Service	□Enable □Disable
Time Server 1	
Time Server 2	
Time Server 3	
Update Rate	
Time Zone	

Move the cursor to **list** for review the SNTP setting.

```
----------------------------------------------------------------------
Status Window...

Time Synchronization Parameters
 Method                    : SNTP v4.0
 Service                   : Enable
 Time Server 1             : ntp-2.vt.edu
 Time Server 2             : ntp.drydog.com
 Time Server 3             : ntp1.cs.wisc.edu
 Update Period             : 3600 secs
 GMT Time Zone Offset       : 8 hours

----------------------------------------------------------------------
```

5.10 Utility

There are three utility tools, upgrade, backup and restore, which embedded in the firmware. You can update the new firmware via TFTP upgrade tools and backup the configuration via TFTP backup tool and restore the configuration via TFTP restore tool. For operation on firmware upgrade and backup or restore the system configuration, you must have your own TFTP server software.

Move the cursor " **>>** " to **utility** and press enter.

```
-------------------------------------------------------------------------------
>> upgrade          Upgrade main software
   backup           Backup system configuration
   Restore          Restore system configuration

-------------------------------------------------------------------------------
```

5.10.1 Upgrade

Move the cursor " **>>** " to **upgrade** and press enter.

```
------------------------------------------------------------------------
 Command: utility upgrade <ip> <file>
 Message: Please input the following information.

 TFTP server IP address (ENTER for default) <192.168.0.2>: 192.168.0.100
 Upgrade filename (ENTER for default) <default.bin>: K5890000.bin

------------------------------------------------------------------------
```

Type TFTP server IP address and upgrade filename of the software.

5.10.2 Backup

Move the cursor " **>>** " to **backup** and press enter.

```
------------------------------------------------------------------------
 Command: utility backup <ip> <file>
 Message: Please input the following information.

 TFTP server IP address (ENTER for default) <192.168.0.2>: 192.168.0.120
 Upgrade filename (ENTER for default) <default.bin>: backup001.bin


------------------------------------------------------------------------
```

Type TFTP server IP address and backup filename of system configuration..

5.10.3 Restore

Move the cursor “ **>>** “ to **restore** and press enter.

```
-----------------------------------------------------------------------
 Command: utility restore <ip> <file>
 Message: Please input the following information.

 TFTP server IP address (ENTER for default) <192.168.0.2>: 192.168.0.150
 Upgrade filename (ENTER for default) <default.bin>: backup002.bin

-----------------------------------------------------------------------
```

Type TFTP server IP address and restore filename of system configuration.

5.11 Exit

If you want to exit the system without saving, use **exit** command to quit system.

```
-----------------------------------------------------------------------
 Command: exit <CR>
 Message: Please input the following information.

 Do you want to disconnect? (y/n):

-----------------------------------------------------------------------
```

Press “y” to confirm the exit operation.

5.12 Setup

All of the setup parameters are located in the subdirectories of setup. Move the cursor “ **>>** “ to **setup** and press enter.

```
-------------------------------------------------------------------------------
>> mode             Switch system operation mode
   shdsl.bis        Configure SHDSL.bis parameters
   wan              Configure WAN interface profile
   bridge           Configure transparent bridging
   vlan             Configure virtual LAN parameters
   stp              Configure bridge STP parameters
   route            Configure routing parameters
   lan              Configure LAN interface profile
   ip_share         Configure NAT/PAT parameters
   firewall         Configure firewall profile
   ip_qos           Configure IP QoS parameters
   dhcp             Configure DHCP parameters
   dns_proxy        Configure DNS proxy parameters
   hostname         Configure local host name
   default          Restore factory default setting

   ----------------------------------------------------------------------------
```

5.12.1 Operation Mode

The product can act as routing mode or bridging mode. The default setting is routing mode. You can change the system operation mode by using mode command. Move the cursor “ **>>** “ to **mode** and press enter.

```
----------------------------------------------------------------------
Command: setup mode <Route|Bridge>
Message: Please input the following information.

System operation mode (TAB select) <Route>: Route
----------------------------------------------------------------------
```

Operation Mode:

Operation Mode	□Route □Bridge

5.12.2 SHDSL.bis

You can setup the SHDSL.bis parameters by the command **shdsl.bis**. Move the cursor “ **>>** “ to shdsl.bis and press enter.

```
-------------------------------------------------------------------------------
`>> mode             Configure SHDSL.bis mode
    link             Configure shdsl.bis link
    n*64             Configure SHDSL.bis data rate
    type             Configure SHDSL.bis annex type
    margin           Configure SHDSL.bis SNR margin
    tcpam            Configure shdsl.bis TCPAM type
    probe            Configure shdsl.bis line probe
    tclayer          Configure shdsl.bis TC Layer
    clear            Clear current CRC error count

-------------------------------------------------------------------------------
```

SHDSL.bis:

Mode	□STU-C □STU-R
Link	□2-Wire □M-Pair □M-Pair(Conexant) □Auto_Fall_Back □Standby □Multi-link
Line rate (Nx64)	
Annex Type	□A □B □AF □BG
SNR Margin	
TCPAM	□Auto □TCPAM-16 □TCPAM-32
Probe	□Disable □Enable
TC Layer	□ATM □EFM

5.12.2.1 Mode

There are two types of SHDSL.bis mode, STU-C and STU-R. STU-C means the terminal of central office and STU-R means customer premise equipment.

5.12.2.2 Link

Notice that this link item is only for 4-wire models.

2-wire mode

For 4-wires model, it can use only the first one pair for the single pair DSL wire application.

M – Pair Mode

In this mode, each wire pairs of SHDSL.bis router must be configured with the same line rate. If one pair fails then the entire line must be restarted. It also has the Conexant M-pair standard used with connection to other router with Conexant chip set solution.

Auto Fall Back Mode

Two DSL pairs are working simultaneously. When one pair of both is disconnect, the other pair will keep working.

Stanby Mode

Only one of two pairs are working, other pair is standby. If the working pair fails, the standby pair will start up to continues.

Multi–Link Mode

For 4-wires model, each pair will connect to two different remote device, which may or may not be in the same location.

*5.12.2.3 N*64*

You can setup the data rate by the multiple of 64Kbps where n is from 3 to 89.

If the router is 4 wire models and doesn't use on 2-wire mode, the line rate will double from 2-wire model's setting.

		2-wire model	4-wire model
Annex A/B	TCPAM-16	192~2304 kbps(n=3~36)	384~4608 kbps(n=6~72)
Annex AF/BG	TCPAM-16	192~3840 kpbs (n=3~60)	384~7680 kbps(n=6~120)
	TCPAM-32	768~5696 kpbs(n=12~89)	1536~11392 kbps(n=24~178)

5.12.2.4 Type

There are four types of SHDSL.bis Annex type, **Annex-A**, **Annex-B**, **Annex-AF**, and **Annex-BG**.

5.12.2.5 Margin

Generally, you cannot need to change SNR margin, which range is from -10 to 21. SNR margin is an index of line connection. You can see the actual SNR margin in STATUS SHDSL.bis. The larger is SNR margin; the better is line connection quality. If you set SNR margin in the field as 3, the SHDSL.bis connection will drop and reconnect when the SNR margin is lower than 3. On the other hand, the device will reduce the line rate and reconnect for better line connection.

5.12.2.6 Tcpam

There are two TCPAM setting on SHDSL.bis: TCPAM-16 or TCPAM-32. In most case, you can set Auto. It can use TCPAM-16 or TCPAM-32 for Annex A/F or B/G. If using Annex A or B, only TCPAM-16 can use.

5.12.2.7 Probe

For adaptive mode, you have to Enable. The router will adapt the data rate according to the line status.

5.12.2.8 TC Layer

There have two TC layer setting on this router: EFM layer and ATM layer. According which networks connected: ATM based access networks or Ethernet based access networks

5.12.2.9 Clear

Clear command can clear CRC error count.

5.12.3 WAN

The router supports 8 PVC, private virtual circuit, and so you can setup eight WAN, such as WAN1 to WAN8. Move the cursor " **>>** " to **wan** and press enter.

For example, to set up WAN1, type **1** on interface number.

```
----------------------------------------------------------------------
Command: setup wan <1~8>
Message: Please input the following information.

Interface number <1~8>: 1
----------------------------------------------------------------------
```

```
>> protocol         Link type protocol
   address          IP address and subnet mask
   vpi_vci          Configure VPI/VCI value
   encap            Configure encapsulation type
   qos              Configure VC QoS
   isp              Configure account name, password and idle time
   ip_type          Configure IP type in PPPoA and PPPoE
   list             WAN interface configuration
```

WAN parameter:

WAN interface number(1~8)		
Protocol	□Disable □Ethernet □PPPoA □IPoA □PPPoE	
Address	IP	
	Mask	
VC	VPI	
	VCI	
Encap	□VC-Mux □LLC	

QoS	□UBR □CBR □rt-VBR □nrt-VBR	
	PCR	
	SCR	
	MBS	
ISP	Name	
	Password	
	Idle Timeout	
IP Type (PPPoA or PPPoE)	□Dynamic □Fixed □Unnumbered	

5.12.3.1 Protocols

There are four types of protocols, IPoA, EoA, PPPoA and PPPoE, which you can setup.

5.12.3.2 IP Address

For dynamic IP of PPPoA and PPPoE, you do not need to setup IP address and subnet mask.

5.12.3.3 VPI VCI

There is an unique VPI and VCI value for Internet connection supported by ISP. The range of VIP is from 0 to 255 and VCI from 0 to 65535.

***VPI** (Virtual Path Identifier) : for set up ATM Permanent Virtual Channels(PVC).*
***VCI** (Virtual Channel Identifier) : for set up ATM Permanent Virtual Channels(PVC).*

5.12.3.4 Ecapsulation

There are two types of encapsulation types, **VC-Mux** and **LLC**.

5.12.3.5 VC QoS

You can setup virtual circuit quality of service, VC QoS, using **qos** command. The router supports **UBR**, **CBR**, **VBR-rt** and **VBR-nrt**. Move the cursor to **qos** and press enter.

```
>> class          Configure QoS class
   pcr            Configure peak cell rate (kbps)
   scr            Configure sustainable cell rate (kbps)
   mbs            Configure max. burst size (cell)
```

UBR (Unspecified Bit Rate) is the simplest service provided by ATM networks. There is no guarantee of anything. It is a primary service used for transferring Internet traffic over the ATM network.

CBR (Constant Bit Rate) is used by connections that requires a static amount of bandwidth that is avilable during the connection life time. This bandwidth is characterized by Peak Cell Rate (PCR). Based on the PCR of the CBR traffic, specific cell slots are assigned for the VC in the schedule table. The ATM always sends a signle cell during the CBR connection's assigned cell slot.

VBR-rt (Varible Bit Rate real-time) is intended for real-time applications, such as compressed voice over IP and video comferencing, that require tightly constrained delays and delay variation. VBR-rt is characterized by a peak cell rate (PCR), substained cell rate (SCR), and maximun burst rate (MBR).

VBR-nrt (Varible Bit Rate non-real-time) is intended for non-real-time applications, such as FTP, e-mail and browsing.

PCR (Peak Cell Rate) in kbps: The maximum rate at which you expect to transmit data, voice and video. Consider PCR and MBS as a menas of reducing lantency, not increasing bandwidth. The range of PCR is 384kbps to 11392kbps

SCR (Substained Cell Rate): The sustained rate at which you expect to transmit data, voice and video. Consider SCR to be the true bandwidth of a VC and not the lone-term average traffic rate. The range of SCR is 384kbps to 11392kbps.

MBS (Maximum Burst Size): The amount of time or the duration at which the router sends at PCR. The range of MBS is 1 cell to 255 cells.

5.12.3.6 ISP

ISP command can configure account name, password and idle time. Idle time is from 0 minute to 300 minutes.

5.12.3.7 IP Type

Most of the ISP use dynamic IP for PPP connection but some of the ISP use static IP. You can configure the IP type: **Dynamic**, **Fixed** and **Unnumbered**. The setting is via **ip_type** command.

The **ip unnumbered** configuration command allows you to enable IP processing on a serial interface without assigning it an explicit IP address. The ip unnumbered interface can "borrow" the IP address of another interface already configured on this router, which conserves network and address space.

5.12.3.8 List

You can review the WAN interface configuration via **list** command.

5.12.4 Bridge

You can setup the bridge parameters in bridge command. If the product is configured as a router, you do not want to setup the bridge parameters.

Move the cursor “ **>>** “ to **bridge** and press enter.

```
-------------------------------------------------------------------------------
>> gateway          Default gateway
   static           Static bridging table
-------------------------------------------------------------------------------
```

5.12.4.1 Gateway

You can setup default gateway IP via gateway command.

Bridge Gateway:

Gateway	

5.12.4.2 Static Bridging Table

You can setup 20 sets of static bridge in static command. After entering **static** menu, the screen will prompt as below:

```
------------------------------------------------------------------------------------------------
>> deny_PCs        Deny PCs to access Internet
   add             Add static MAC entry
   delete          Delete static MAC entry
   modify          Modify static MAC entry
   list            Show static bridging table
------------------------------------------------------------------------------------------------
```

You can deny PCs to access Internet for security purpose use **deny_PCs** command.

After enter **add** menu, the screen will prompt as follow

```
------------------------------------------------------------------------------------------------
>> mac             Configure MAC address
   lan_port        Configure LAN interface bridging type
   wan1_port       Configure WAN1 interface bridging type
   wan2_port       Configure WAN2 interface bridging type
   wan3_port       Configure WAN3 interface bridging type
   wan4_port       Configure WAN4 interface bridging type
   wan5_port       Configure WAN5 interface bridging type
   wan6_port       Configure WAN6 interface bridging type
   wan7_port       Configure WAN7 interface bridging type
   wan8_port       Configure WAN8 interface bridging type

------------------------------------------------------------------------------------------------
```

Deny PCs to access interface:

Deny PCs to access Interface	□Disable □Enable

Static MAC Address:

MAC entry number (1~20)	
MAC Address	
LAN	□Filter □Forward □Dynamic
WAN1	□Filter □Forward □Dynamic
WAN2	□Filter □Forward □Dynamic
WAN3	□Filter □Forward □Dynamic
WAN4	□Filter □Forward □Dynamic
WAN5	□Filter □Forward □Dynamic
WAN6	□Filter □Forward □Dynamic
WAN7	□Filter □Forward □Dynamic
WAN8	□Filter □Forward □Dynamic

5.12.5 VLAN

Virtual LAN (VLAN) is defined as a group of devices on one or more LANs that are configured so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLAN is based on logical instead of physical connections, it is extremely flexible.

You can setup the Virtual LAN (VLAN) parameters in **vlan** command. The router support the implementation of VLAN-to-PVC only for bridge mode operation, i.e., the VLAN spreads over both the COE and CPE sides. The unit supports up to 8 active VLANs with shared VLAN learning (SVL) bridge out of 4096 possible VLANs specified in IEEE 802.1Q.

Move the cursor " **>>** " to **vlan** and press enter.

```
--------------------------------------------------------------------------------
>> mode              Trigger virtual LAN function
   modify            Modify virtual LAN rule
   pvid              Modify port default VID
   link_mode         Modify port link type
   List              Show VLAN configuration

--------------------------------------------------------------------------------
```

To active the VLAN function, move the cursor " **>>** " to **mode** and press enter. The products support two types of VLAN: **802.11q** and **Port-Based**.

```
----------------------------------------------------------------------
Command: setup vlan active <Disable|8021Q|Port>
Message: Please input the following information.

Tigger VLAN function (Tab select) <Disable>: 8021Q
----------------------------------------------------------------------
```

VLAN Mode:

VLAN Mode	□Disable □802.1Q Tag VLAN □Port Based VLAN

The IEEE 802.1Q defines the operation of VLAN bridges that permit the definition, operation, and administration of VLAN topologies within a bridged LAN infrastructure. Port-Based VLANs are VLANs where the packet forwarding decision is based on the associated ports. If you don't use VLAN ,set to **Disbale**.

5.12.5.1 802.11Q VLAN

To modify the VLAN rule, move the cursor " **>>** " to modify and press enter.

```
----------------------------------------------------------------------
Command: setup vlan modify <1~8> <1~4094> <string>
Message: Please input the following information.

Rule entry index <1~8>: 1
VLAN ID (ENTER for default) <1>: 10
VLAN port status (ENTER for default)<111111111>:111111111
```

```
----------------------------------------------------------------------
```

For each VLAN, VID(VLAN ID) and PVID is a unique number among 1~4094.

		1	2	3	4	5	6	7	8	9
No.	VID	LAN	WAN1	WAN2	WAN3	WAN4	WAN5	WAN6	WAN7	WAN8
1										
2										
3										
4										
5										
6										
7										
8										
PVID										
Link Type		□Access □Trunk	□Access □Trunk	□Access □Trunk	□Access □Trunk	□Access □Trunk	□Access □Trunk	□Access □Trunk	□Access □Trunk	□Access □Trunk

To assign PVID (Port VID), move the cursor “>>” to **pvid** and press enter. The port index 1 represents LAN and ports index 2 to 9 represents WAN1 to WAN8 respectively. VID value is the group at which you want to assign the PVID of the port.

```
----------------------------------------------------------------------
Command: setup vlan pvid <1~9> <1~4094>
Message: Please input the following information.

Port index <1~9>: 1
VID Value (Enter for default) <10>: 10
----------------------------------------------------------------------
```

VLAN port status is a 9-digit binary number whose bit-1 location indicates the VLAN port membership in which 1MSB and 8MSBs represents one LAN port and eight WAN ports, respectively. For example, the setting ”vlan modify 1 20 111000000” means that the VID 20 member ports includes LAN, WAN1 and WAN. The member ports are tagged members. Use PVID command to change the member port to untagged members

To modify the link type of the port, move the cursor to **link_mod**e and press enter. There are two types of link: **access** and **trunk**. **Trunk** link will send the tagged packet form the port and **Access** link will send un-tagged packet form the port. The port index 1 represents LAN and ports index 2 to 9 represents WAN1 to WAN8 respectively. According to the operation mode of the device, link type of WAN port is automatically configured. If the product operates in bridge mode, the WAN link type will be trunk, and in routing mode, access.

```
----------------------------------------------------------------------
Command: setup vlan link_mode <1~12> <Access|Trunk>
Message: Please input the following information.

Port index <1~12>: 1
Port link type (Tab select) <Trunk>: Access
----------------------------------------------------------------------
```

5.12.5.2 Port Based VLAN

With port-based VLAN, the port is assigned to a specific VLAN independent of the user or system attached to the port. This means all users attached to the port should be members in the same VLAN. The port based setting performs the VLAN assignment. The port configuration is static and cannot be automatically changed to another VLAN without manual reconfiguration.

For Port Based VLAN, user must set up the table using 802.11Q methods. But don’t care the value of VID , PVID or link type.

Port Based VLAN:

No.	LAN1	WAN1	WAN2	WAN3	WAN4	WAN5	WAN6	WAN7	WAN8
1									
2									
3									
4									
5									
6									
7									
8									

To view the VLAN table, move the cursor to **list** and press enter.

5.12.6 STP

Spanning-Tree Protocol (STP) is a link management protocol that provides path redundancy while preventing undesirable loops in the network. For an Ethernet network to function properly, only one active path can exist between two stations

The default is disable.

```
------------------------------------------------------------------------------------------------
>> active           Trigger Bridge STP function

------------------------------------------------------------------------------------------------
```

STP:

STP Function	□Disable □Enable

Once you enable the STP feature, you can see the STP status will follow IEEE 802.1d standard to work. The working steps are Blocking, Listening, Learning and forwarding.

5.12.7 Route

You can setup the routing parameters in route command. If the product is configured as a bridge, you do not want to setup the route parameters. Move the cursor “ **>>** “ to **route** and press enter.

```
>> static          Configure static routing table
   rip             Configure RIP protocol

```

5.12.7.1 Static

If the Router is connected to more than one network, it may be necessary to set up a static route between them. A static route is a pre-determined pathway that network information must travel to reach a specific host or network.

With Dynamic Routing, you can enable the Router to automatically adjust to physical changes in the network’s layout. The Router, using the RIP protocol, determines the network packets’ route based on the fewest number of hops between the source and the destination. The RIP protocol regularly broadcasts routing information to other routers on the network.

You can setup 20 sets of static route in static command. After entering **static** menu, the screen will show as follow:

```
>> add             Add static route entry
   delete          Delete static route entry
   List            Show static routing table

```

You can add 20 sets of static route entry by using **add** command. Type the IP information of the static route including IP address, subnet mask and gateway.

Static Route Table:

	IP Address	Subnet Mask	Gateway
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			

20			

You can delete the static route information via **delete** command.

You can review the static route entry by using **list** command.

5.12.7.2 Rip

To configure Routing Information Protocol (RIP), you can use **rip** command to setup the parameters. Move the cursor “**>>**” to **rip** and press enter.

```
--------------------------------------------------------------------------------
>> generic          Configure operation and auto summery mode
   lan              Configure LAN interface RIP parameters
   wan              Configure WAN interface RIP parameters
   list             Show RIP configuration

--------------------------------------------------------------------------------
```

Generic RIP Parameters

Generic command can setup RIP mode and auto summery mode.

Generic RIP Parameter:

Rip Mode	□Disable □Enable
Auto Summary	□Disable □Enable

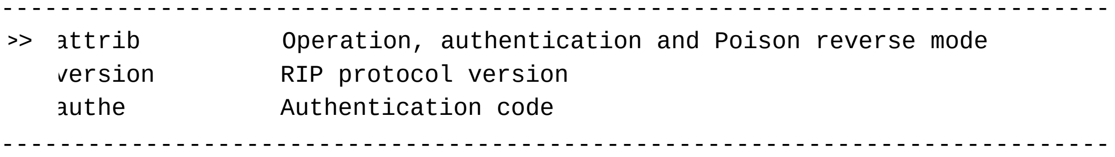
Interface RIP Parameters

[LAN]

If there are any routers in your LAN, you can configure LAN interface RIP parameters via **lan** command.

```
-----------------------------------------------------------------------------
 Command: setup route rip lan <1~1> <more...>
 Message: Please input the following information.

 Active interface number <1~1>:
 -----------------------------------------------------------------------------
```

The screen will prompt as follow:



```
-----------------------------------------------------------------------------
>>  attrib          Operation, authentication and Poison reverse mode
    version         RIP protocol version
    authe           Authentication code
-----------------------------------------------------------------------------
```

[WAN1 ~ WAN8]

The product supports 8 PVCs and you can configure the RIP parameters of each WAN via **wan** command. Move the cursor “**>>**” to **wan** and press enter.

```
----------------------------------------------------------------------
Command: setup route rip wan <1~8> <more...>
Message: Please input the following information.
```

```
Active interface number <1~8>: 1
----------------------------------------------------------------------
```

The screen will prompt as follow:

```
>> attrib           Operation, authentication and Poison reverse mode
   version          RIP protocol version
   authe            Authentication code
```

Attrib command can configure RIP mode, authentication type and Poison reverse mode.
Version command can configure RIP protocol version.
Authe command can configure authentication code.

Interface RIP Parameter:

Interface	(LAN, WAN1~8)
RIP Mode	□Disable □Enable □Silent
Authentication type	□None □Password □MD5
Poison reverse mode	□Disable □Enable
RIP protocol version	□Ver.1 □Ver.2
Authentication code	

You can review the list of RIP parameters via **list** command.

5.12.8 LAN

LAN interface parameters can be configured LAN IP address, subnet mask and NAT network type.

```
-------------------------------------------------------------------------------
 Command: setup lan <1~1> <more...>
 Message: Please input the following information.

 Interface number <1~1>:1
 ------------------------------------------------------------------------------
```

There are only one LAN port, so type 1 and press ENTER.

```
-----------------------------------------------------------------------------
>> ip_type           IP type
   address           LAN IP address and subnet mask
   attrib            NAT network type
   Ethernet          Media type

----------------------------------------------------------------------------
```

Ip_type can set up this IP is **Fixed** or **Dynamic**.
Address can set up **IP address** and **subnet mask**.
Attrib can set up NAT network type: **Global** or **Virtual**.
Ethernet item can set up the PHY parameters on this LAN port: **Auto**, **100M-Full**, **100M-Half**, **10M-Full** and **10M-Half**.

LAN Port parameter:

IP Type	□Fixed □Dynamic
LAN IP Address	
LAN Subnet Mask	
NAT Network type	□Global □Virtual
Ethernet Media Type	□Auto □100M-Full □100M-Half □10M- Full □10M-Half

5.12.9 IP share

You can configure Network Address Translation (NAT), Port Address Translation (PAT) and Demilitarized Zone (DMZ) parameters in **ip_share** menu.

5.12.9.1 NAT

NAT (Network Address Translation) is the translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network. One network is designated the inside network and the other is the outside. Typically, a company maps its local inside network addresses to one or more global outside IP addresses and reverse the global IP addresses of incoming packets back into local IP addresses. This ensure security since each outgoing or incoming request must go through a translation process, that also offers the opportunity to qualify or authenticate the request or match it to a previous request. NAT also conserves on the number of global IP addresses that a company needs and lets the company to use a single IP address of its communication in the Internet world.

To configure Network Address Translation (NAT), Move the cursor "**>>**" to **ip_share** then press enter.

```
-------------------------------------------------------------------------------
>> nat               Configure network address translation
   pat               Configure port address translation
   dmz               Configure DMZ host function

-------------------------------------------------------------------------------
```

Virtual IP address pool

You can configure NAT parameters in **nat** menu.

```
-------------------------------------------------------------------------------
>> virtual           Virtual IP address pool
   global            Global IP address pool
   Fixed             Fixed IP address mapping

-------------------------------------------------------------------------------
```

The **virtual** menu contains range of virtual IP address, delete virtual IP address, and show virtual IP address.

```
-------------------------------------------------------------------------------
>> range             Edit virtual IP address pool
   delete            Delete virtual IP address pool
   List              Show virtual IP address pool

-------------------------------------------------------------------------------
```

You can create five virtual IP address pool range in **range** command.

```
----------------------------------------------------------------------
Command: setup ip_share nat virtual range <1~5> <ip> <1~253>
Message: Please input the following information.

NAT local address range entry number <1~5>: 1
Base address: 192.168.0.2
Number of address: 49
----------------------------------------------------------------------
```

NAT (Virtual IP address and range)

	Base Address	Number of Address
1		
2		
3		
4		
5		

You can delete virtual IP address range- from 1 to 5- by using **delete** command.

You can view the virtual IP address range via **list** command.

Global IP address pool

To setup global IP address pool, move the cursor "**>>**" to **global** command and press enter.

```
----------------------------------------------------------------------------------------------------
>> range            Edit global IP address pool
   interface        Bind address pool to specific interface
   delete           Delete global IP address pool
   list             Show global IP address pool

----------------------------------------------------------------------------------------------------
```

You can create five global IP address pool range via **range** command.

```
----------------------------------------------------------------------
Command: setup ip_share nat global range <1~5> <ip> <1~253>
Message: Please input the following information.

NAT global IP address range entry number <1~5>: 1
Base address: 122.22.22.2
Number of address: 3
----------------------------------------------------------------------
```

After configuration global IP address range, you can bind address pool to specific interface via **interface** command.

NAT (Global IP Address and range):

	Base Address	Number of Address	Active Interface Numbe(1~8)
1			
2			
3			
4			
5			

```
----------------------------------------------------------------------
Command: setup ip_share nat global interface <1~5> <1~8>
Message: Please input the following information.

NAT global ddress range entry number <1~5>: 1
Active interface number <1~8>: 1
----------------------------------------------------------------------
```

You can delete global IP address range- from 1 to 5- by using **delete** command.

You can view the global IP address range via **list** command.

Fixed IP address mapping

To modify fixed IP address mapping, move the cursor “**>>**” to **fixed** command and press enter.

```
   virtual         Virtual IP address pool
   global          Global IP address pool
>> Fixed           Fixed IP address mapping
```

```
>> modify          Modify fixed NAT mapping
   interface       Bind address pair to specific interface
   delete          Delete fixed NAT mapping
   list            Show fixed IP address mapping
```

You can create up to 10 fixed NAT mapping entry via **modify** command.

```
----------------------------------------------------------------------
Command: setup ip_share nat fixed modify <1~10> <ip> <ip>
Message: Please input the following information.

Fixed NAT mapping entry number <1~10>: 1
Local address: 192.168.0.250
Global address: 122.22.22.2
----------------------------------------------------------------------
```

Fixed Address Mapping:

	Local Address	Global Address
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

After configuration fixed IP address entry, you can bind the entry to specific interface via **interface** command.

```
----------------------------------------------------------------------
Command: setup ip_share nat fixed interface <1~10> <1~8>
Message: Please input the following information.

Fixed NAT mapping entry number <1~10>: 1
Active interface number (Enter for default) <1~8>: 1
----------------------------------------------------------------------
```

Fixed NAT Mapping:

Mapping entry number	Active Interface number(1~8)
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	

You can delete fixed NAT mapping entry from 1 to 10 by using **delete** command.

You can view the fixed NAT mapping entry via **list** command.

5.12.9.2 PAT

Port Address Translation (PAT) is a feature of a device that translates TCP or UDP communications made between hosts on a private network and hosts on a public network. It allows a single public IP address to be used by many hosts on the private network, which is usually called a Local Area Network or LAN.

A PAT device transparently modifies IP packets as they pass through it. The modifications make all the packets which it sends to the public network from the multiple hosts on the private network appear to originate from a single host - the PAT device - on the public network.

In PAT, both the sender's private IP and port number are modified; the PAT device chooses the port numbers which will be seen by hosts on the public network.

In PAT there is generally only one publicly exposed IP address and incoming packets from the public network are routed to their destinations on the private network by reference to a table held within the PAT device which keeps track of public and private port pairs. This is often called connection tracking.

To configure Port Address Translation, move the cursor “**>>**” to **pat** and press enter.

```
--------------------------------------------------------------------------------------------------------
>> clear            Clear virtual server mapping
   modify           Modify virtual server mapping
   list             Show virtual server mapping pool

--------------------------------------------------------------------------------------------------------
```

You can delete virtual server mapping entry- from 1 to 10- by using **clear** command.

You can create up to 10 virtual server mapping entry via **modify** command.

```
----------------------------------------------------------------------
Command: setup ip_share pat modify <1~10> <more...>
Message: Please input the following information.

Virtual server entry number <1~10>: 1
----------------------------------------------------------------------
```

After key in enter, the screen will prompt as below.

```
-------------------------------------------------------------------------------
>> interface       Active interface
   port            TCP/UDP port number
   server          Host IP address and port number
   protocol        Transport protocol
   name            Service name
   begin           The schedule of beginning time
   end             The schedule of ending time

-------------------------------------------------------------------------------
```

Set the active interface number via **interface** command.

You can configure the global port number by using **port** command.

The local server, host, IP address and port number are configured via **server** command.

The authorized access protocol is setup via **protocol** command.

Name command can be used to configure the service name of the host server.

Begin and **end** command is used to setup the local server schedule to access.

Virtual Server:

Virtual Server entry number(1~10)	
Interface(1~8)	
ICP/UDP Port Number(1~65534)	
Host IP Address	
Host Port Number	
Protocol	□TCP □UDP
Service Name	
Beginning Time	
Ending Time	

You can view the fixed NAT mapping entry via **list** command.

5.12.9.3 DMZ

DMZ (demilitarized zone) is a computer host or small network inserted as a “neutral zone” between a company private network and the outside public network. It prevents outside users from getting direct access to a server that has company private data.

To setup demilitarized zone, move the cursor “>>” to **dmz** and press enter.

```
-------------------------------------------------------------------------------
>> active           Tigger DMZ host function
   address          Configure virtual IP address and interface

-------------------------------------------------------------------------------
```

You can enable the demilitarized zone via **active** command.

After enabling the DMZ, shift the cursor to **address** and press enter.

```
----------------------------------------------------------------------
Command: setup ip_share dmz address <ip> <1~8>
Message: Please input the following information.

Virtual IP address: 192.168.0.251
Active interface number (Enter for default) <1>: 1
----------------------------------------------------------------------
```

DMZ Host:

DMZ Host Function	□Disable □Enable
IP Address	Active interface number
	1
	2
	3
	4
	5
	6
	7
	8

5.12.10 Firewall

Notices that this item is only for firewall models.
To configure Firewall, move the cursor “ >> “ to **firewall** and press enter.

```
----------------------------------------------------------------------
>> level             Configure firewall security level
   pkt_filter        Configure packet filter
   dos_protect       Configure DoS protect
----------------------------------------------------------------------
```

5.12.10.1 firewall security level

There are three level of firewall, which you can setup in this product.

Level one, **basic**, only enables the NAT firewall and the remote management security. The NAT firewall will take effect if NAT function is enabled. The remote management security is default to block any WAN side connection to the device. Non-empty legal IP pool in ADMIN will block all remote management connection except those IPs specified in the pool.

Level two, **automatic**, enables basic firewall security and all DoS protection.

Level three, **advanced**, is an advanced level of firewall where user can determine the security level for special purpose, environment, and applications by configuring the DoS protection and defining an extra packet filter with higher priority . Note that, an improper filter policy may degrade the capability of the firewall and/or even block the normal network traffic.

The firewall security level can configure via **level** command.

Firewall Security Level:

Level	□Basic □Automatic □Advanced

5.12.10.2 Packet Filtering

Packet filtering function can be configured by **pkt_filter** command. Move the cursor to **pkt_filter** and press enter.

```
>> active           Tigger packet filtering function
   drop_flag        Drop fragment packets
   add              Add packet filtering rule
   delete           Delete packet filtering rule
   modify           Modify packet filtering rule
   exchange         Exchange the filtering rule
   list             Show packet filtering table
```

To enable the packet filtering function, you can use **active** command.
To enable the drop fragmented packets, you can use **drop_frag** command.

Function enable:

Packet filtering function	□Disable □Enable
Drop fragmented packet	□Disable □Enable

Add the packet filtering rule via **add** command.
You can set up maximum 32 numbers packet filtering rules, Anytime you can modify and exchange their rules by using **modify** and **exchange** command.

```
>> protocol         Configure protocol type
   direction        Configure direction mode
   src_ip           Configure source IP parameter
   dest_ip          Configure destination IP parameter
   port             Configure port parameter (TCP and UDP only)
   tcp_flag         Configure TCP flag (TCP only)
```

```
icmp_type       Configure ICMP flag (ICMP only)
description     Packet filtering rule description
enable          Enable the packet filtering rule
begin           The schedule of beginning time
end             The schedule of ending time
action          Configure action mode
```

Packet filtering:

Protocol	□ANY □TCP □UDP □ICMP □GRE □RSVP □ESP □AH
Direction	□Inbound □Outbound
Source IP	
Destination IP	
Source Port	(TCP/UDP only)
Destination Port	(TCP/UDP only)
TCP flag	(TCP only) □ANY □SYN □ACK
ICMP flag	(ICMP only) □Echo_Reply □Dest_Unreach □Src_Quench □Redirect □Echo_Request □R_Advertise □R_Solicit □T_Exceed □Param_Problem □T_Stamp □T_Stamp_Reply □Info_Request □Info_Reply □Addr_Mask_Request □Addr_Mask_Reply
Description	
Enable	□ON □OFF
Begin Time	
End Time	
Action	□DENY □PERMIT

5.12.10.3 DoS Protection

DoS protection parameters can be configured in dos_protection menu.
Move the cursor to **dos_protection** and press enter.

```
>> syn_flood       Enable protection SYN flood attack
   icmp_flood      Enable protection ICMP flood attack
   udp_flood       Enable protection UDP flood attack
   ping_death      Enable protection PING of death attack
   land_attack     Enable protection land attack
   ip_spoff        Enable protection IP spoofing attack
   smurf_attack    Enable protection smurf attack
   fraggle_attack  Enable protection fraggle attack
```

SYN flood: A SYN flood is a form of denial-of-service attack, attempts to slow your network by requesting new connections but not completing the process to open the connection. Once the buffer for these pending connections is full a server will not accept any more connections and will be unresponsive.

ICMP flood: A sender transmits a volume of ICMP request packets to cause all CPU resources to be consumed serving the phony requests.

UDP Flood: A UDP flood attack is a denial-of-service (DoS) attack using the User Datagram Protocol(UDP). A sender transmits a volume of requests for UDP diagnostic services which cause all CPU resources to be consumed serving the phony requests.

Ping of Death: A ping of death (POD) attack attempts to crash your system by sending a fragmented packet, when reconstructed is larger than the maximum allowable size.

Land attack: A land attack is an attempt to slow your network down by sending a packet with identical source and destination addresses originating from your network.

IP Spoofing: IP Spoofing is a method of masking the identity of an intrusion by making it appeared that the traffic came from a different computer. This is used by intruders to keep their anonymity and can be used in a Denial of Service attack.

Smurf attack: The Smurf attack is a way of generating a lot of computer network traffic to a victim host. That is a type of denial-of-service attack. A Smurf attack involves two systems. The attacker sends a packet containing a ICMP echo request (ping) to the network address of one system. This system is known as the amplifier. The return address of the ping has been faked (spoofed) to appear to come from a machine on another network (the victim). The victim is then flooded with responses to the ping. As many responses are generated for only one attack, the attacker is able use many amplifiers on the same victim.

Fraggle attack: A Fraggle attack is a type of denial-of-service attack where an attacker sends a large amount of UDP echo traffic to IP broadcast addresses, all of it having a fake source address. This is a simple rewrite of the smurf attack code.

DoS Protection

SYN flood	□Disable □Enable	Packets per sec. 0~700	
ICMP flood	□Disable □Enable	Packets per sec. 0~700	
UDP flood	□Disable □Enable	Packets per sec. 0~700	
PING of death	□Disable □Enable		

Land	□Disable □Enable
IP_spoofing	□Disable □Enable
Smurf	□Disable □Enable
Fraggle	□Disable □Enable

5.12.11 IP QoS

The Internet has worked so far with a best effort traffic model: every packet is treated (forwarded or discarded) equally. This is very simple and efficient model and several arguments have been stated against any need for a more complicated system.

To configure IP QoS , move the cursor “ >> “ to **ip_qos** and press enter.

```
-----------------------------------------------------------------------
>> active           Trigger IP QoS function
   add              Add IP QoS policy
   delete           Delete IP QoS policy
   modify           Modify IP QoS policy
   list             Show IP QoS policy table
-----------------------------------------------------------------------
```

You can enable the IP QoS function via **active** command.

The add parameters of IP QoS can be configured via **add** command

To delete the policy is configured by **delete** command.

To modify the policy is configured by **modify** command.

You can view the IP QoS configuration via **list** command.

When use the **add** command, it will show the following:

```
--------------------------------------------------------------------------------------------------------
>> Protocol        Configure protocol
   local_ip        Configure local IP parameter
   remote_ip       Configure remote IP parameter
   Port            Configure port parameter
   description     Policy description
   Enable          Enable the policy
   Precedence      Configure precedence parameter

--------------------------------------------------------------------------------------------------------
```

Protocol identifier: One can differentiate IP from other network level protocols using link level information - TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

Source port number: The only way to identify applications run over TCP or UDP is to look for port numbers and compare them to list of well-known port numbers. While in most cases the mapping is correct there are many cases when some service or client uses a port reserved for an another application.

Destination port number: The destination port identifies traffic originating from the client to the server.

Source host address: It **c**an identify the end system sending data and based on that classify traffic

Destination host address: It can identify the end system receiving data.

Command	Description
Protocol	Set up the port protocol type (ANY, TCP or UDP)
Local_ip	Configure the local IP address
Remote_ip	Configure the remote IP address
Port	Configure the local port and remote port range
Description	Define the description of policy
Enable	Enable the policy
Precedence	Define the priority of the policy

IP QoS:

Protocol	□ANY □TCP □UDP
Local IP	
Remote IP	
Local Port	
Remote Port	
Description	
Enable	□ON □OFF
Precedence	(0 ~ 5)

5.12.12 DHCP

Dynamic Host Configuration Protocol (DHCP) is a communication protocol that lets network administrators to manage centrally and automate the assignment of Internet Protocol (IP) addresses in an organization's network. Using the Internet Protocol, each machine that can connect to the Internet needs a unique IP address. When an organization sets up its computer users with a connection to the Internet, an IP address must be assigned to each machine.

Without DHCP, the IP address must be entered manually at each computer. If computers move to another location in another part of the network, a new IP address must be entered. DHCP lets a network administrator to supervise and distribute IP addresses from a central point and automatically sends a new IP address when a computer is plugged into a different place in the network.

To configure DHCP server, move the cursor “ >> “ to **dhcp** and press enter.

```
--------------------------------------------------------------------------------
>> generic          DHCP server generic parameters
   fixed            DHCP server fixed host IP list
   relay            DHCP relay parameter
   list             Show DHCP configuration

--------------------------------------------------------------------------------
```

5.12.12.1 DHCP Server generic

The generic DHCP parameters can be configured via **generic** command.

```
--------------------------------------------------------------------------------
>> active           Trigger DHCP server function
   gateway          Default gateway for DHCP client
   netmask          Subnet mask for DHCP client
   ip_range         Dynamic assigned IP address range
   lease_time       Configure max lease time
   name_server1     Domain name server1
   name_server2     Domain name server2
   name_server3     Domain name server3

--------------------------------------------------------------------------------
```

Command	Description
Active	Trigger DHCP server function
Gateway	Configure default gateway for DHCP client
Net mask	Configure subnet mask for DHCP client
IP range	Configure dynamic assigned IP address range.
Lease time	Set up dynamic IP maximum lease time
Name server 1	Set up the IP address of name server #1
Name server 2	Set up the IP address of name server #2
Name server 3	Set up the IP address of name server #3

DHCP Server:

DHCP Server	□Disable □Enable
DHCL Client gateway	
DHCP Client Netmask	
Start IP address	
Address Range	
Lease Time	
Name Server 1 IP	
Name Server 2 IP	
Name Server 3 IP	

5.12.12.2 DHCP Server Fixed Host

Fixed Host IP Address list are setup via **fixed** command.

```
--------------------------------------------------------------------------------
>> add              Add a fixed host entry
   delete           Delete a fixed host entry
--------------------------------------------------------------------------------
```

```
    ------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------
```

When use the fixed host entry, you must enter the MAC address and IP address as the same time. There can be set up to 10 maximum fixed host IP address.

DHCP Server with Fixed Host:

	Mac Address	IP Address
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

5.12.12.3 DHCP Relay

Active the DHCP relay and remote server IP address via **relay** command

```
-----------------------------------------------------------------------------
 Command: setup dhcp relay <Disable|Enable> <ip>
 Message: Please input the following information.

 Parameter of command 'relay' (TAB Select) <Disable>: Enable
 IP address (ENTER for default) <192.168.0.124>:

 -----------------------------------------------------------------------------
```

DHCP Relay:

DHCP Relay	□Disable □Enable
IP Address	

You can view the full DHCP configuration via **list** command.

5.12.13 DNS proxy

The Domain Name Service (DNS) is a system designed to allow the identification of Internet servers to be based on names rather than IP addresses. Because Internet communication is based on IP addresses, all names must be translated into an IP address. This is the purpose of a Domain Name Server.

Enter the IP address of DNS proxy use DNS proxy command. Move cursor " **>>** " to **dns_proxy** and press enter.

```
----------------------------------------------------------------------
Command: setup dns_proxy <IP> [IP] [IP]
```

```
Message: Please input the following information.

DNS server 1 (ENTER for default) <168.95.1.1>: 10.0.10.1
DNS server 2: 10.10.10.1
DNS server 3:
----------------------------------------------------------------------
```

You can setup three DNS servers in the router. The number 2 and 3 DNS servers are option.

DNS Server IP:

DNS Server 1 IP	
DNS Server 2 IP	
DNS Server 3 IP	

5.12.14 Host name

A Host Name is the unique name by which a network-attached. The hostname is used to identify a particular host in various forms of electronic communication.

Enter local host name via hostname command. Move cursor “ **>>** “ to **hostname** and press enter.

```
----------------------------------------------------------------------
Command: setup hostname <name>
Message: Please input the following information.

Local hostname (ENTER for default) <SOHO>: test
----------------------------------------------------------------------
```

The host name can’t use more than 15 characters and don’t use space character.

Some of the ISP requires the Host Name as identification. You may check with ISP to see if your Internet service has been configured with a host name. In most cases, this field can be ignored.

Host Name:

Host Name	

5.12.15 Default

If you want to restore factory default, first move the cursor “ >> “ to **default** and then press enter.

```
----------------------------------------------------------------------
Command: setup default <name>
Message: Please input the following information.

Are you sure? (Y/N): y
----------------------------------------------------------------------
```

Press “y” to confirm the restore factory setting operation.